



Rocking the Pocket Book: Hacking Chemical Plants for Competition and Extortion

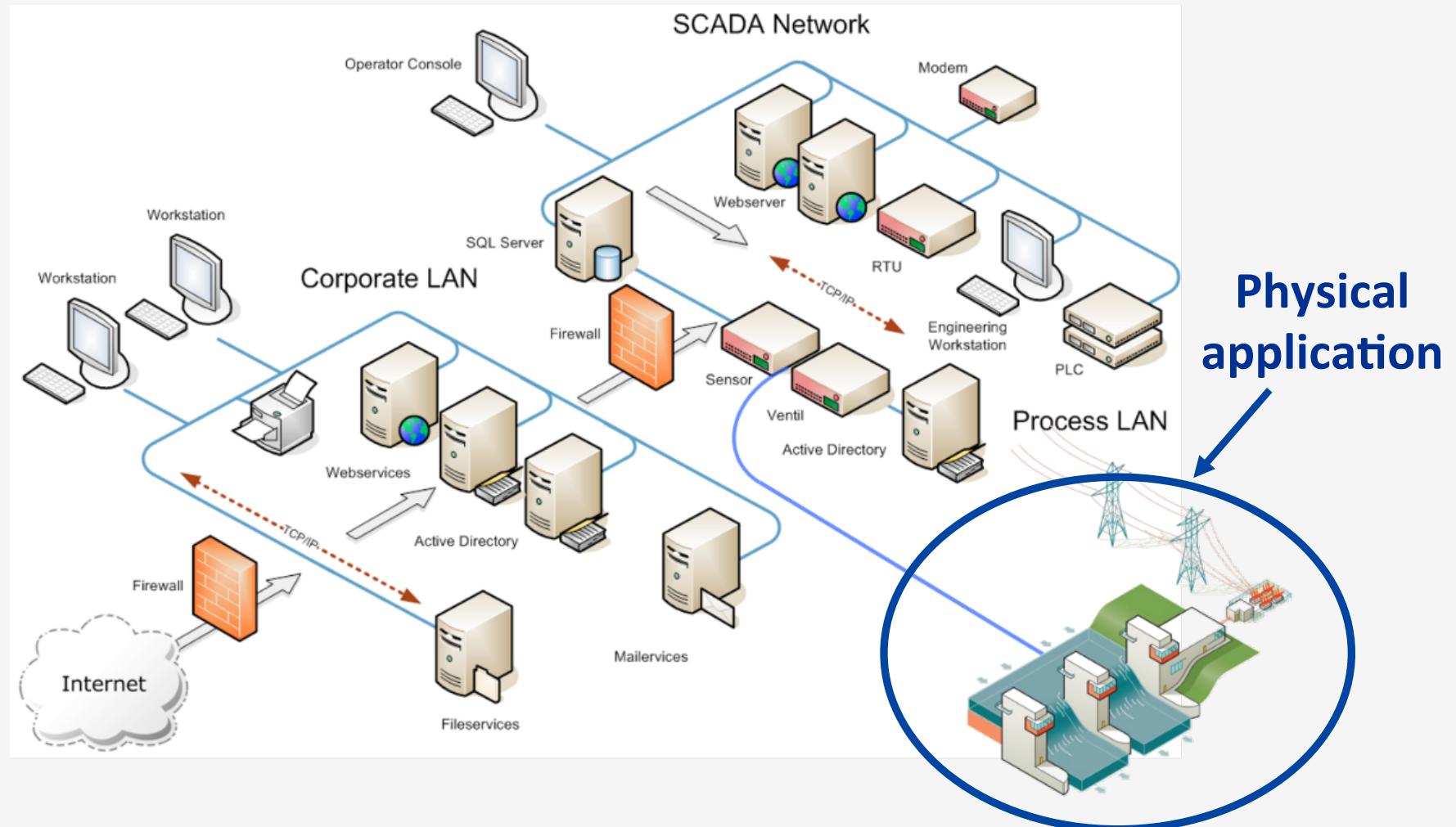
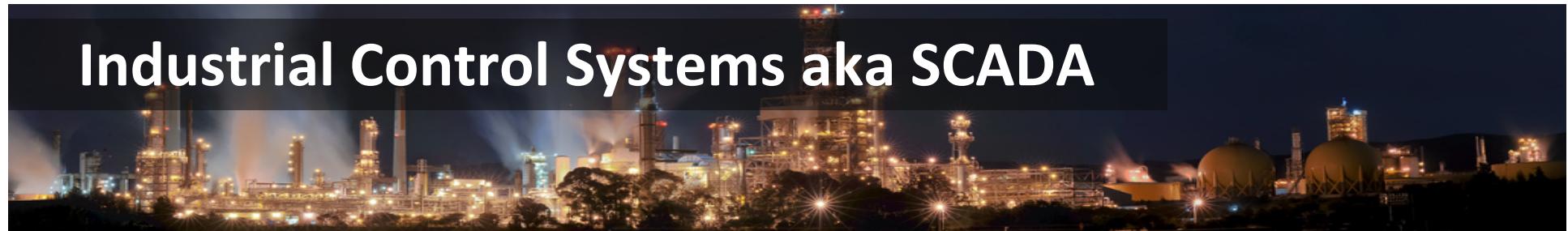
Marina Krotofil

**HITB Singapore
14.10.2015**

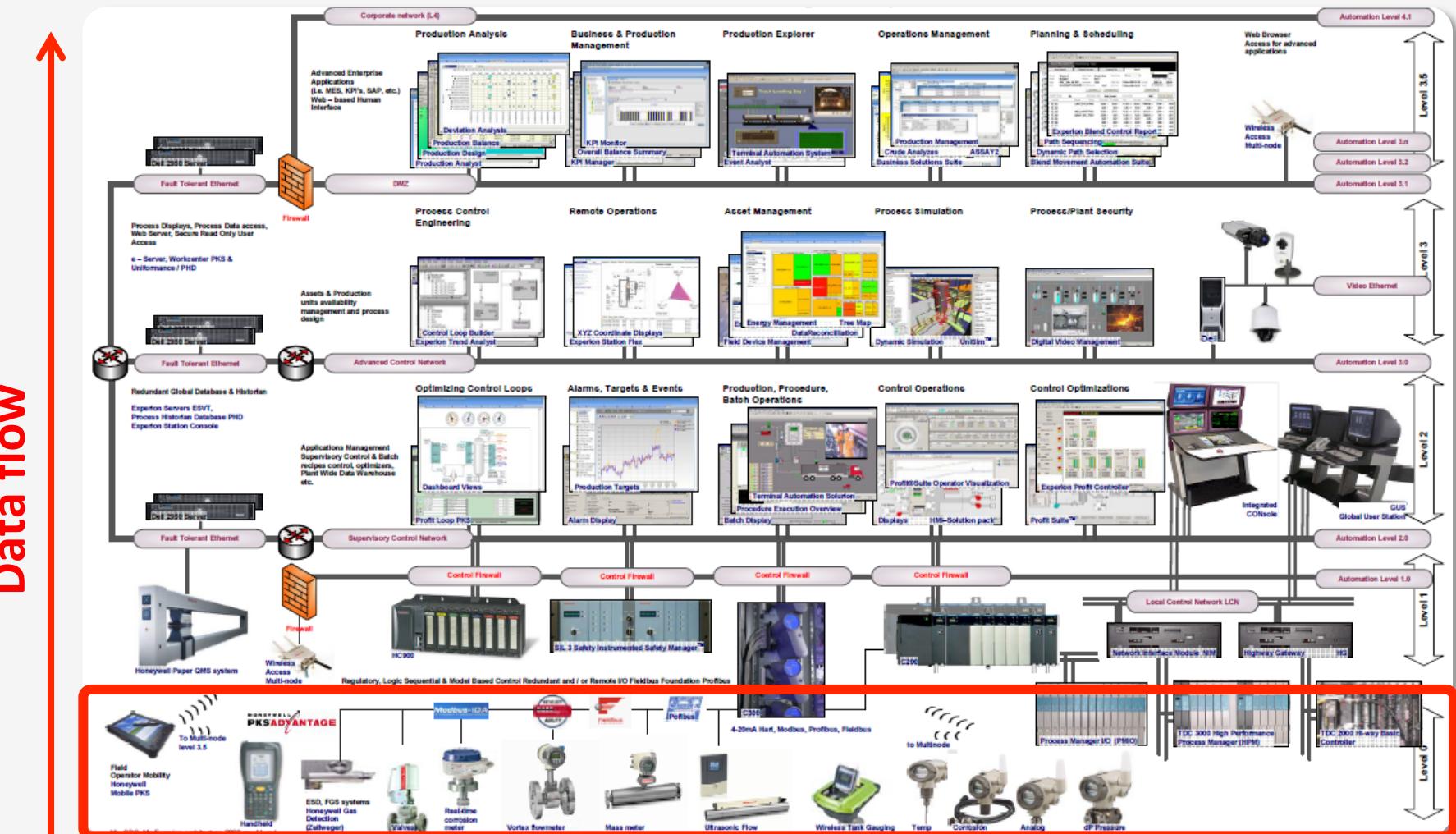


HEAVY METALS

Industrial Control Systems aka SCADA



Industrial Control Systems aka SCADA



Physical process

Cyber-physical systems

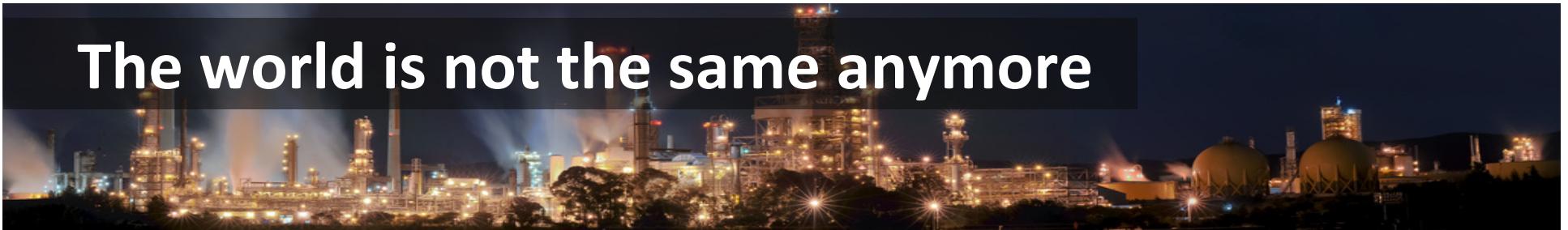


Cyber-physical systems are IT systems “embedded” in an application in the physical world

Interest of the attacker is in the physical world



The world is not the same anymore



James Bond 007 –
Casino Royale

Pity!!



James Bond 007 – Skyfall

Cyber-physical hack

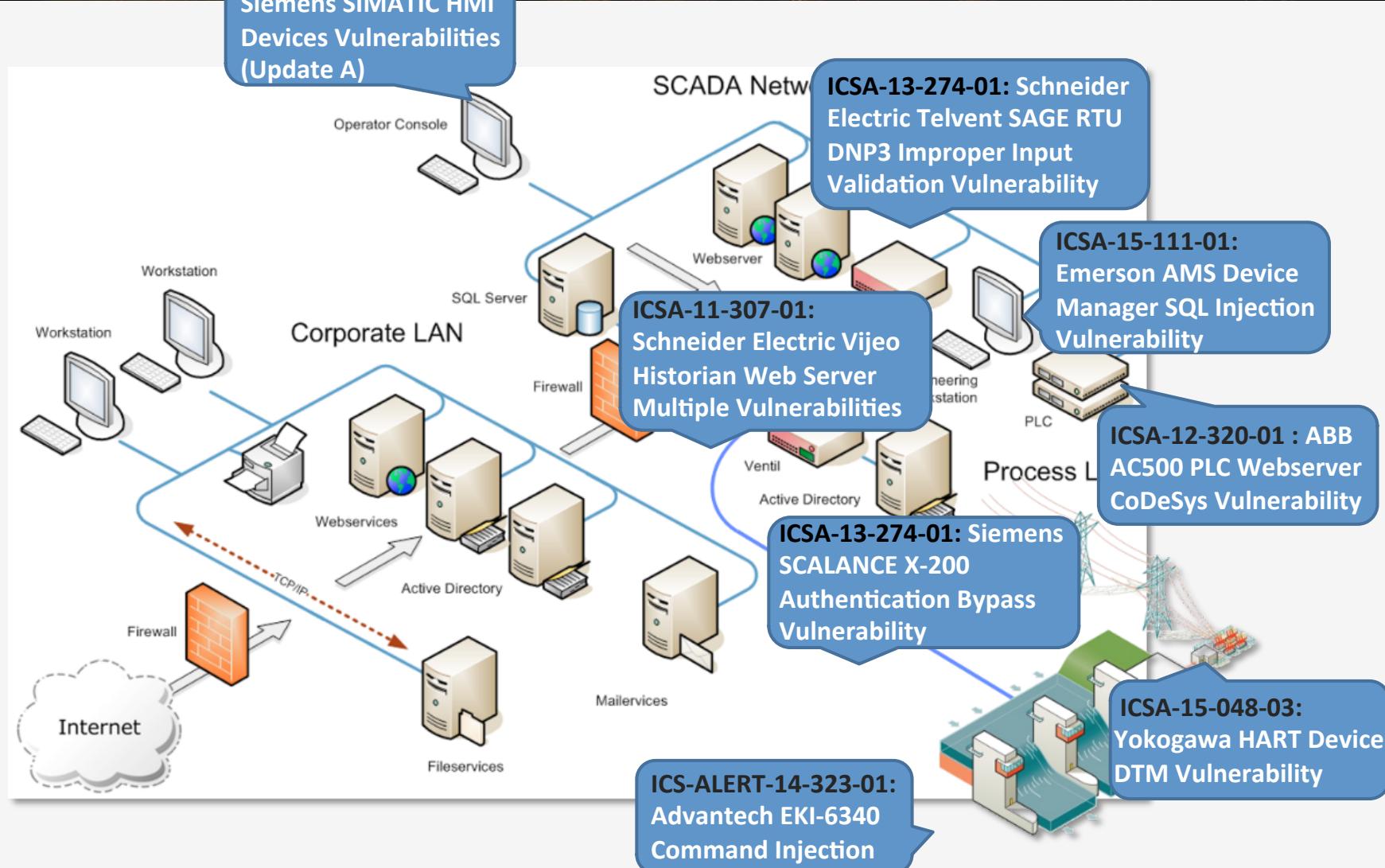
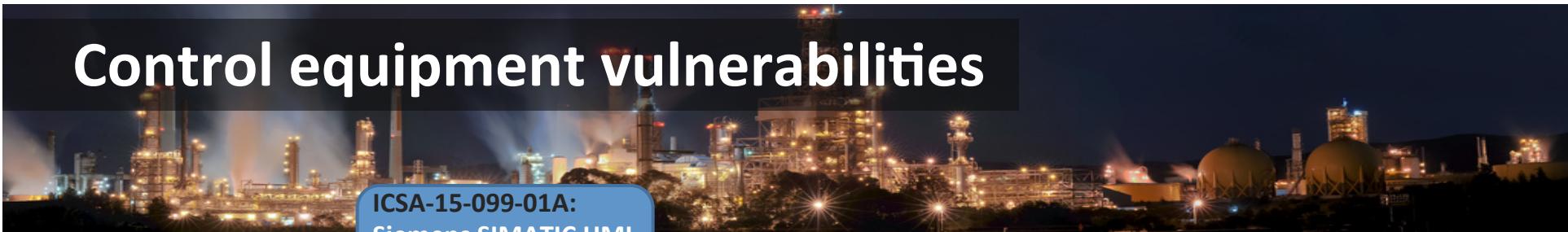


James Bond 007: Skyfall



Control systems security

Control equipment vulnerabilities



ICS-CERT recommendation



ICSA-13-274-01: Siemens SCALANCE X-200 Authentication Bypass Vulnerability

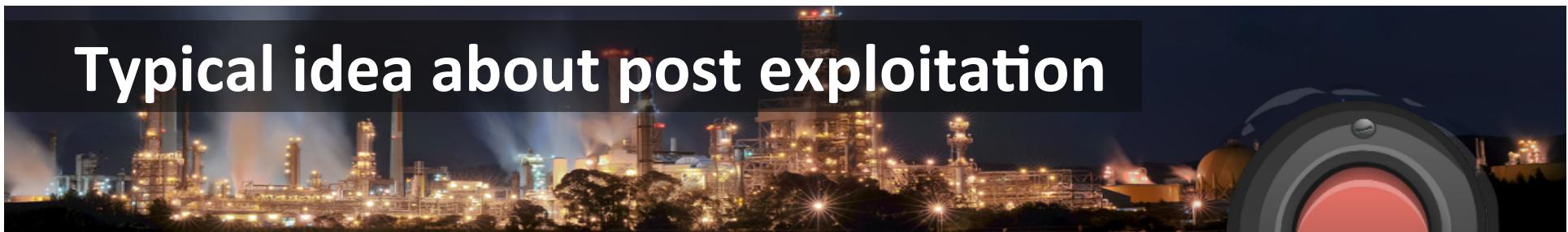
IMPACT

Successful exploitation of this vulnerability may allow attackers to perform administrative operations over the network without authentication.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.



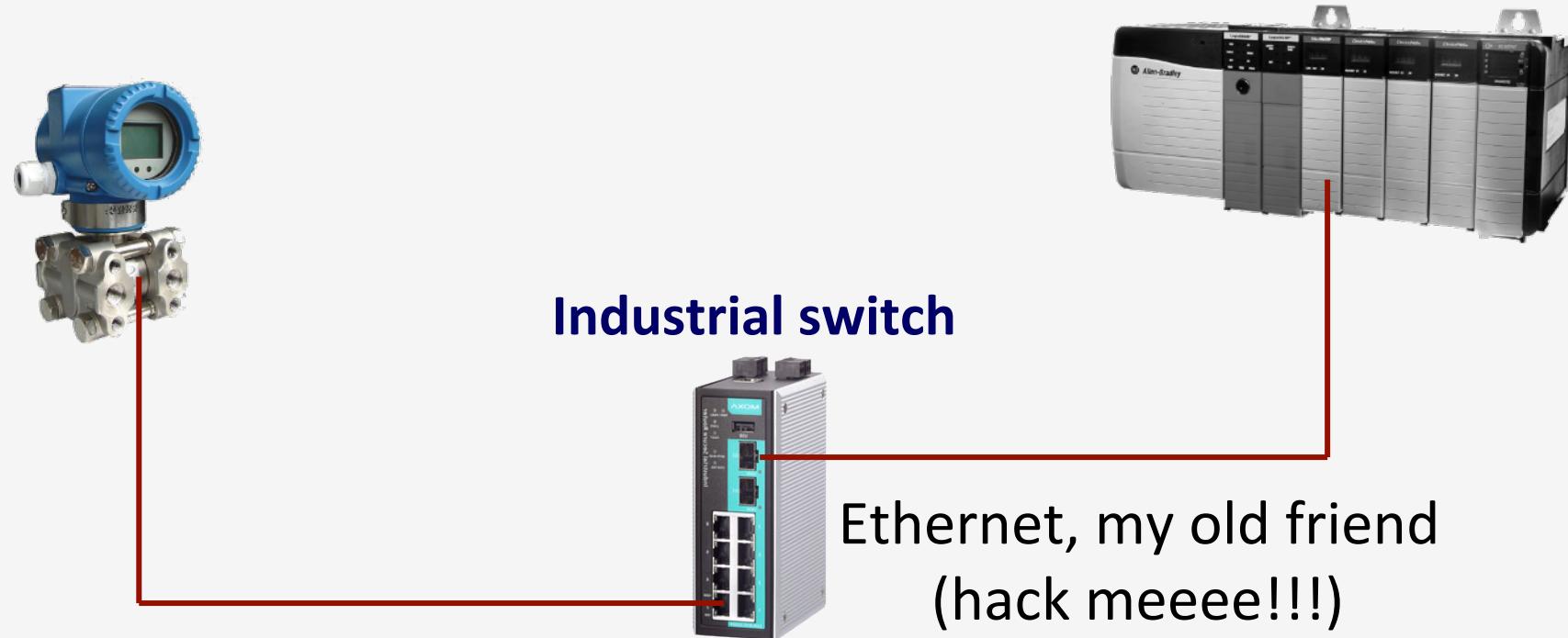
Typical idea about post exploitation



magic button
(does not exist!)



TCP/IP based communication



Modbus, DNP, IEC850 are common protocols

Here is the plant. What is the plan?

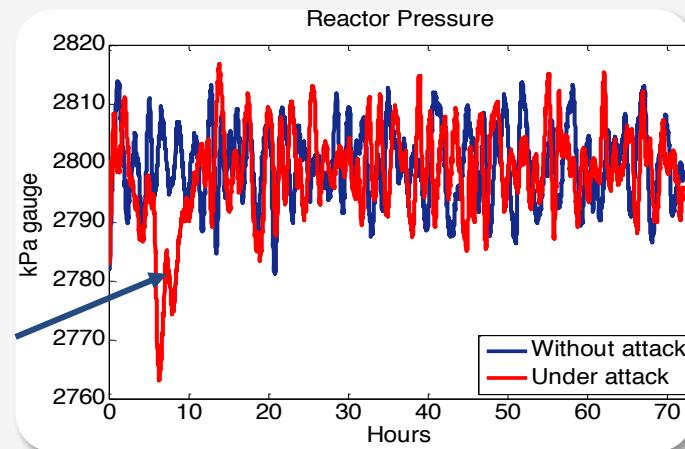


Source: simentari.com

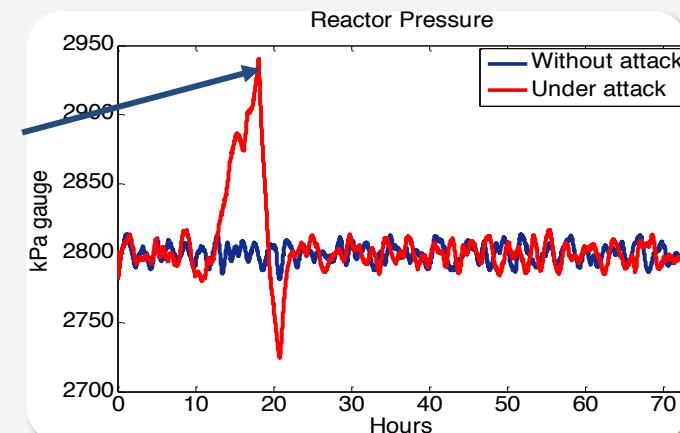
Timing of the DoS attack



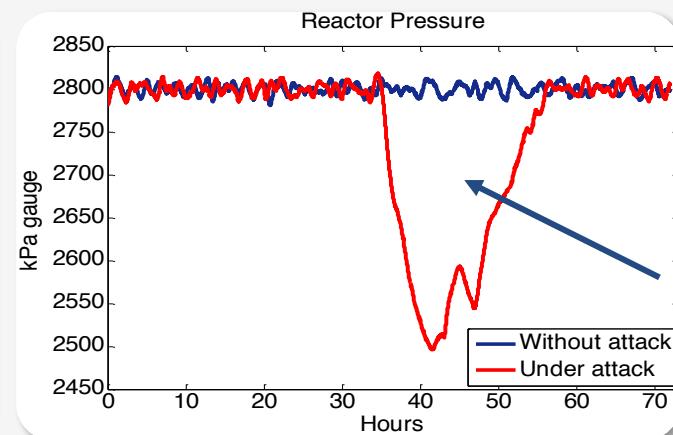
Ordinary
glitch



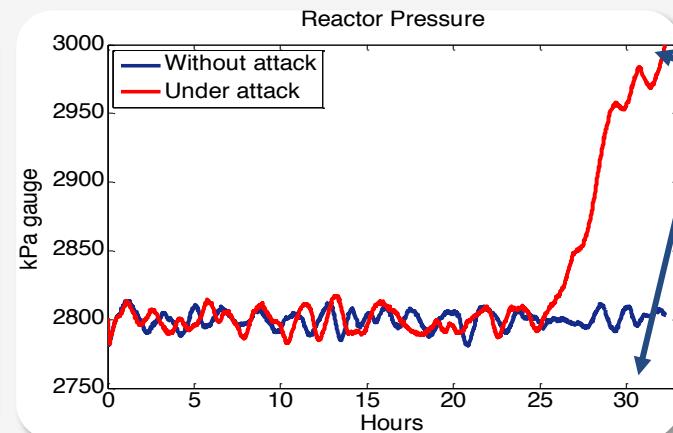
Near miss
(almost
safety
accident)



Economic
inefficiency



Safety
shutdown



Impact of 8h long attack on reactor pressure at random time

Impact evaluation



- What exactly the attacker can do with the vulnerability?
- Any further necessary conditions required?
- How severe the potential physical impact?



Answering these questions requires understanding how the attacker interacts with the control system and the process

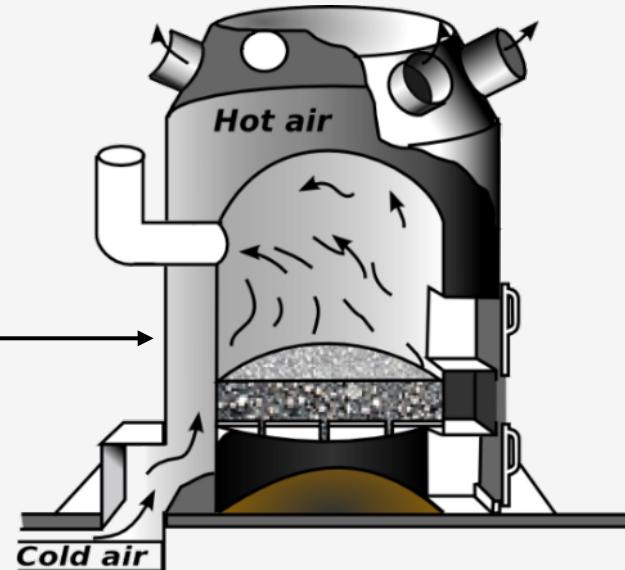


Process control

Process control automation

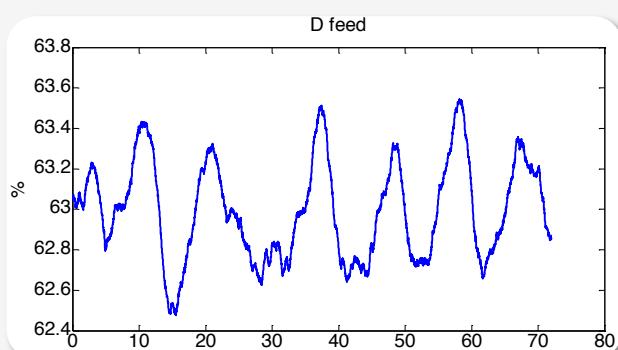
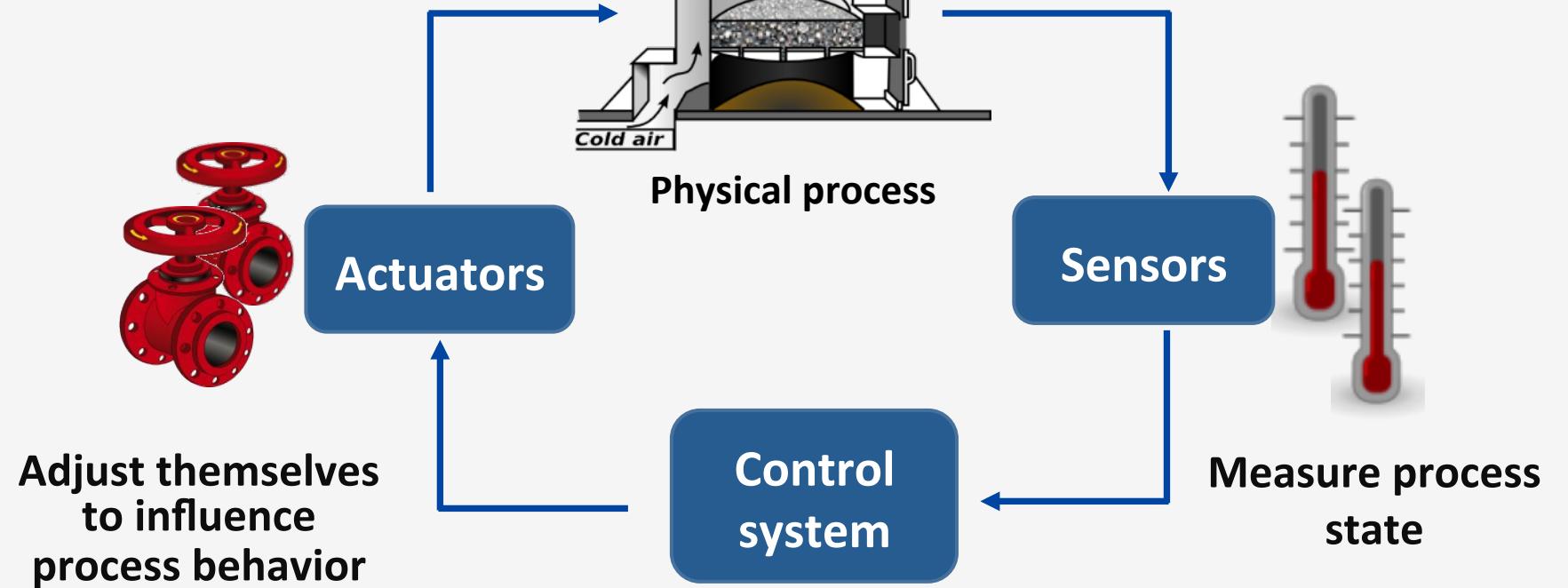


Set point

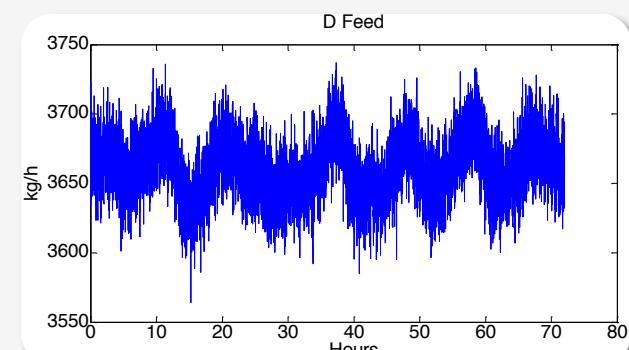


Running downstairs to turn on the furnace every time it gets cold is tiring, so you automate it with a thermostat

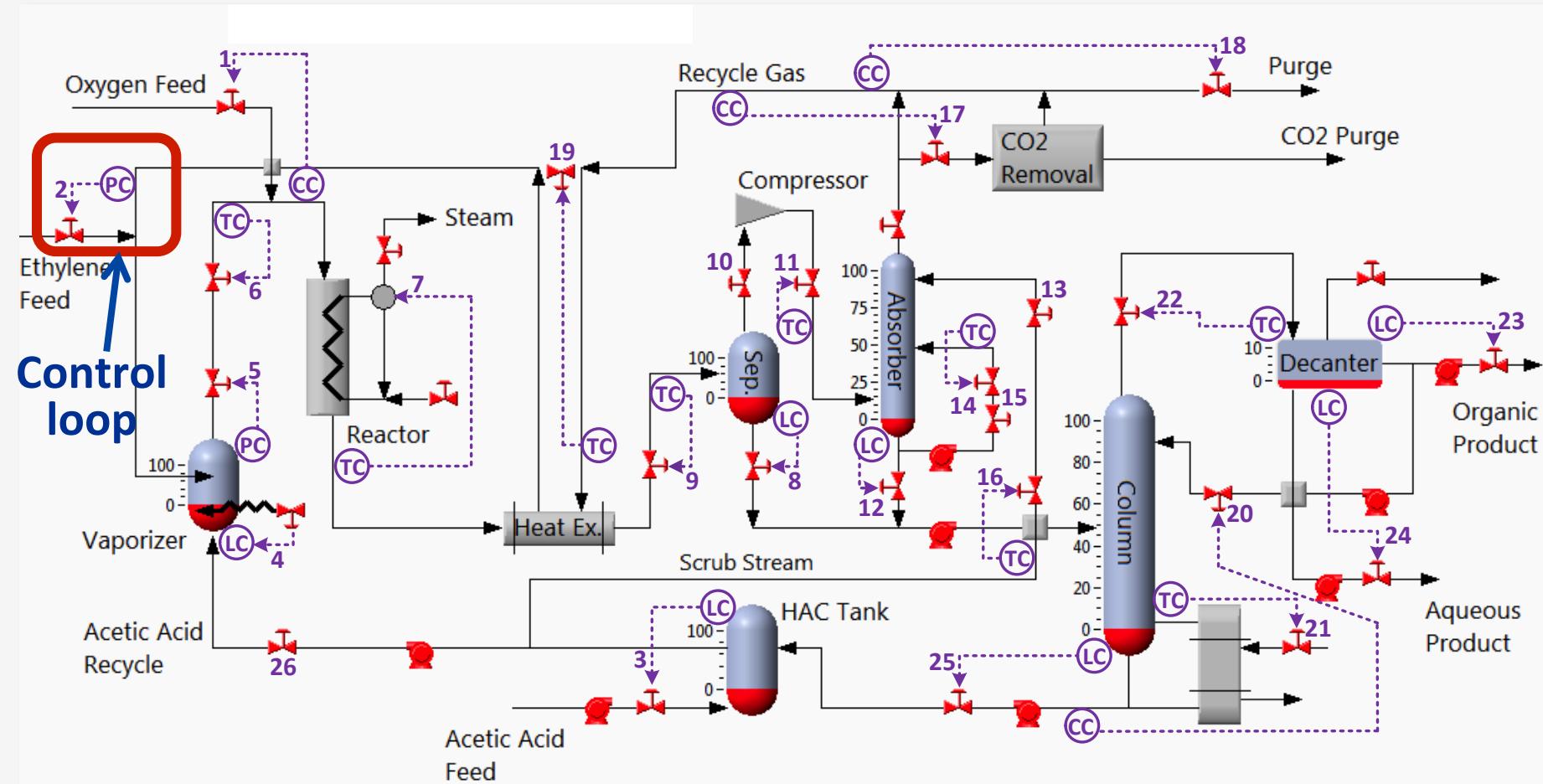
Control loop



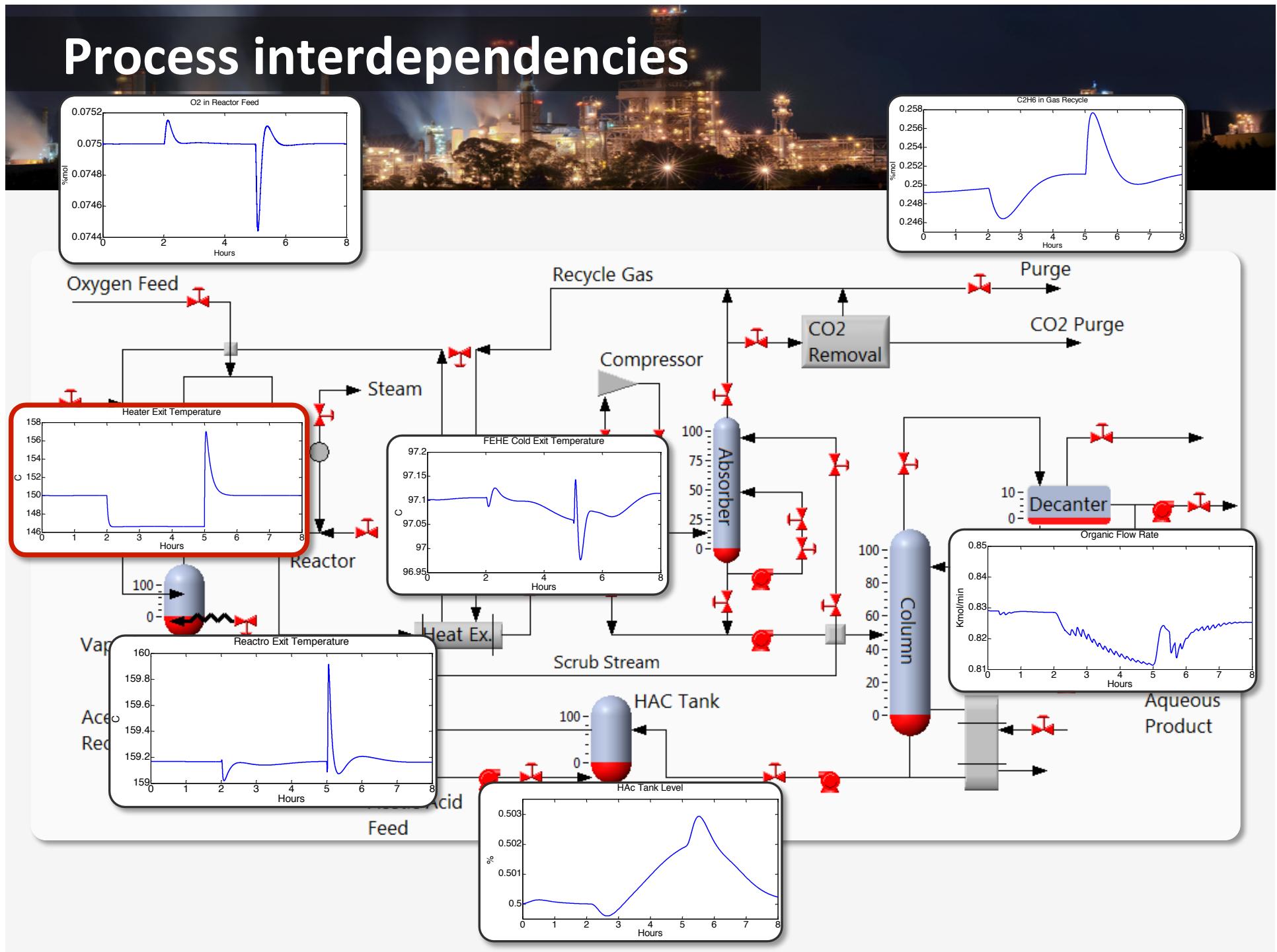
Computes control commands for actuators



Understanding control structure



Process interdependencies



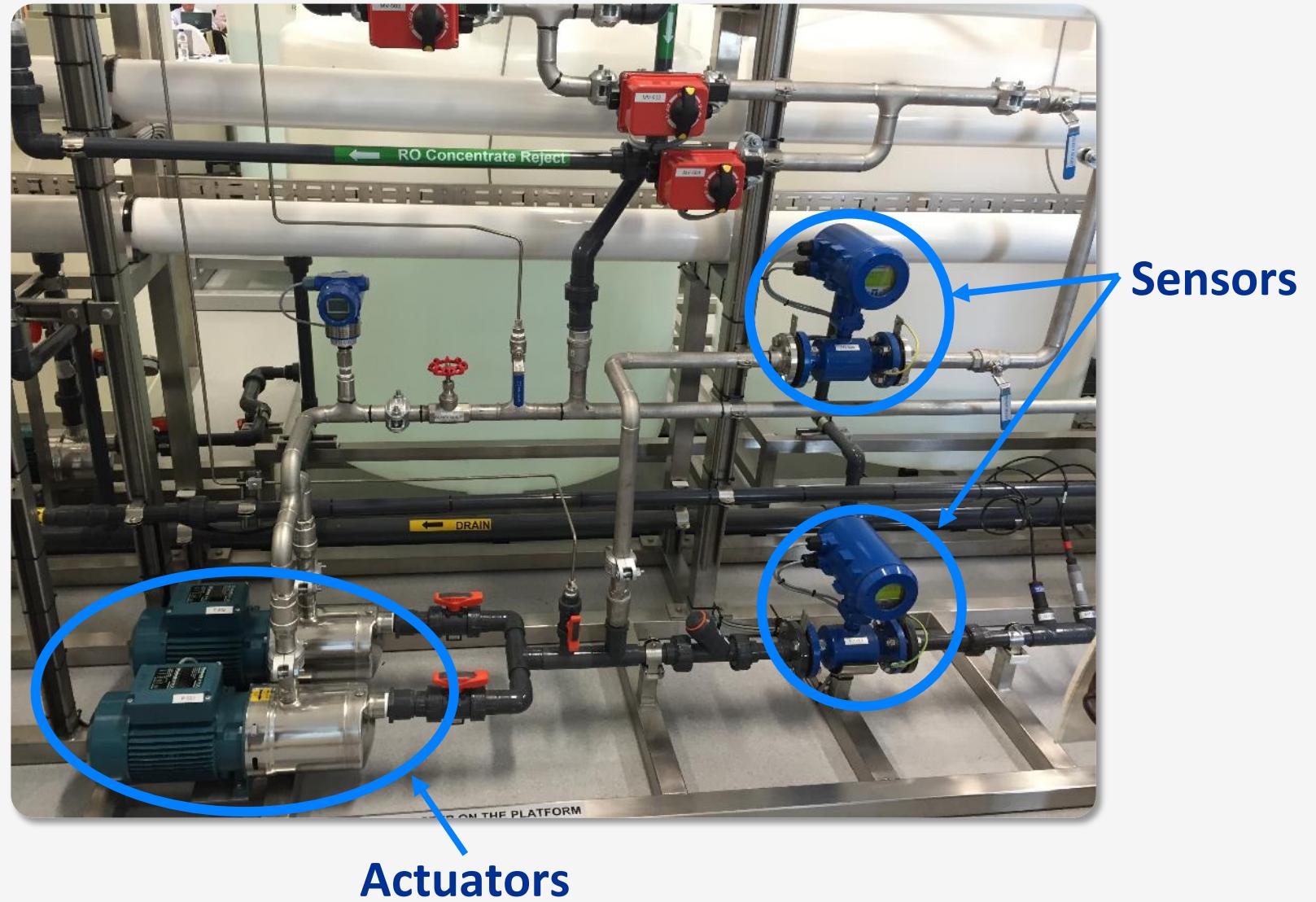
Control equipment



- ❑ In large –scale operations control logic gets more complex than a thermostat
- ❑ The control is typically done by a programmable logic controller (PLC)



Plant floor



Field communication



PLC

Wires to the process

Wires are run from sensors and actuators into wiring cabinets

PLC internals

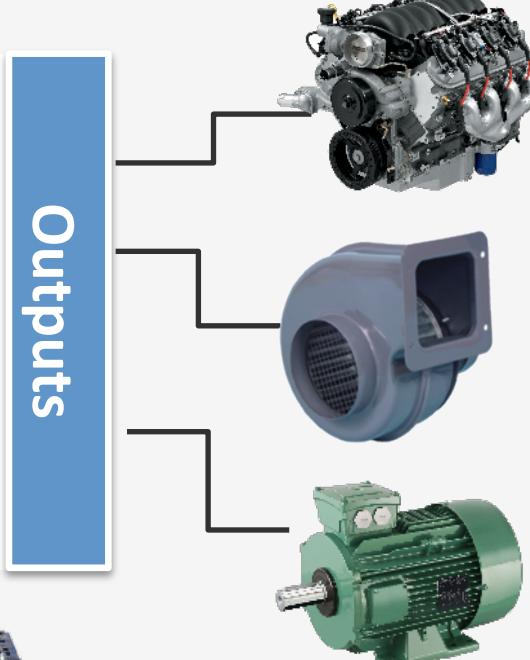


Sensors



1. Copy data from inputs to temporary storage
2. Run the logic
3. Copy from temporary storage to outputs

Actuators



Inputs



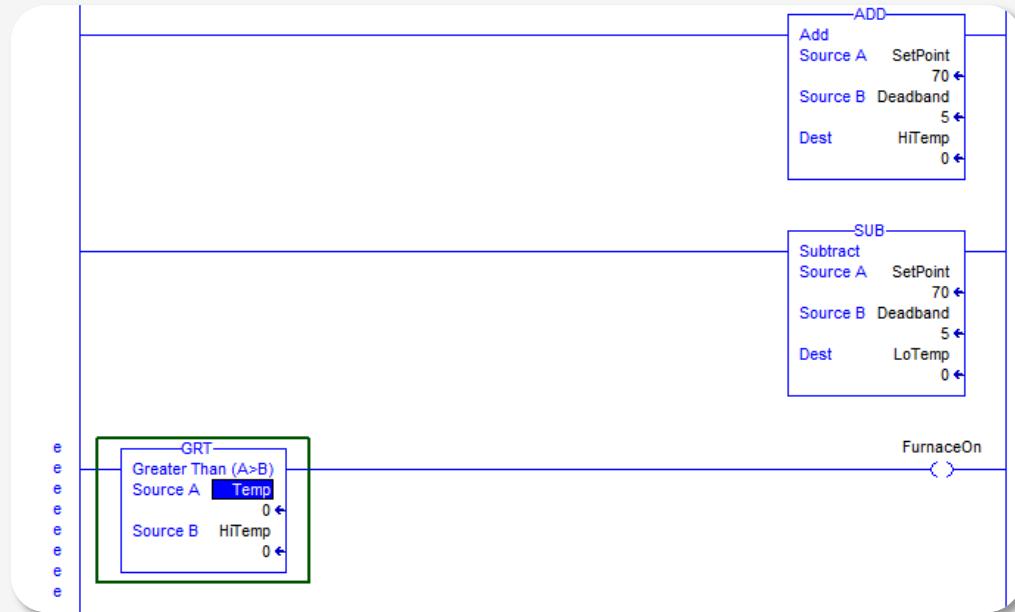
Outputs



Control logic



- Defines what should (not) happen to the process:
conditions, order, time



(Programmed graphically most
of time. Nope, no python or
java)

If tank pressure in PLC 1 > 1800
reduce inflow in PLC 3

Interlocks

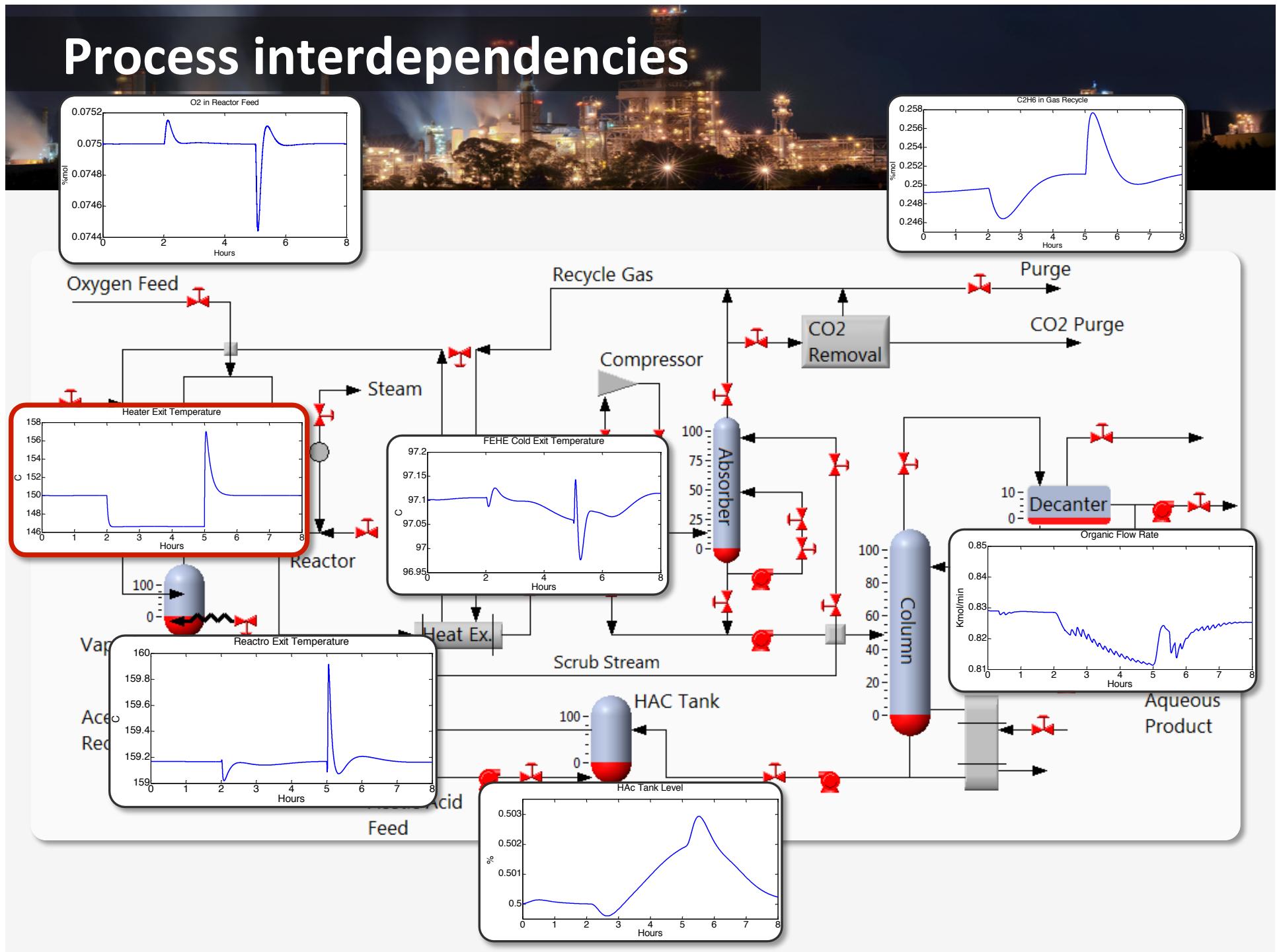


- Process safety increasingly depends on the logic in the controllers
- Ladder logic can tell you a lot about what the engineer that designed the process was worried about
- Search for the master stop

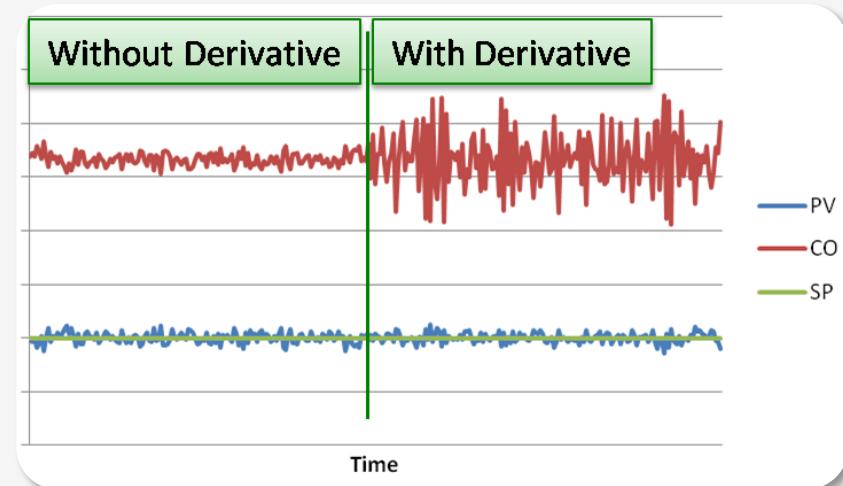
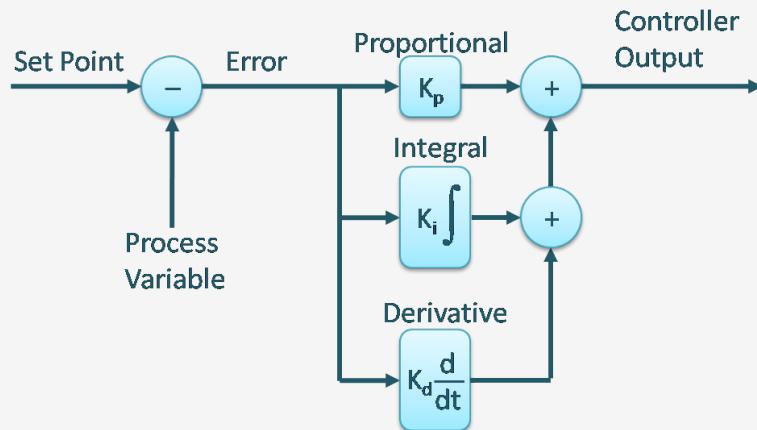


The motor should not be running when the valve is closed

Process interdependencies



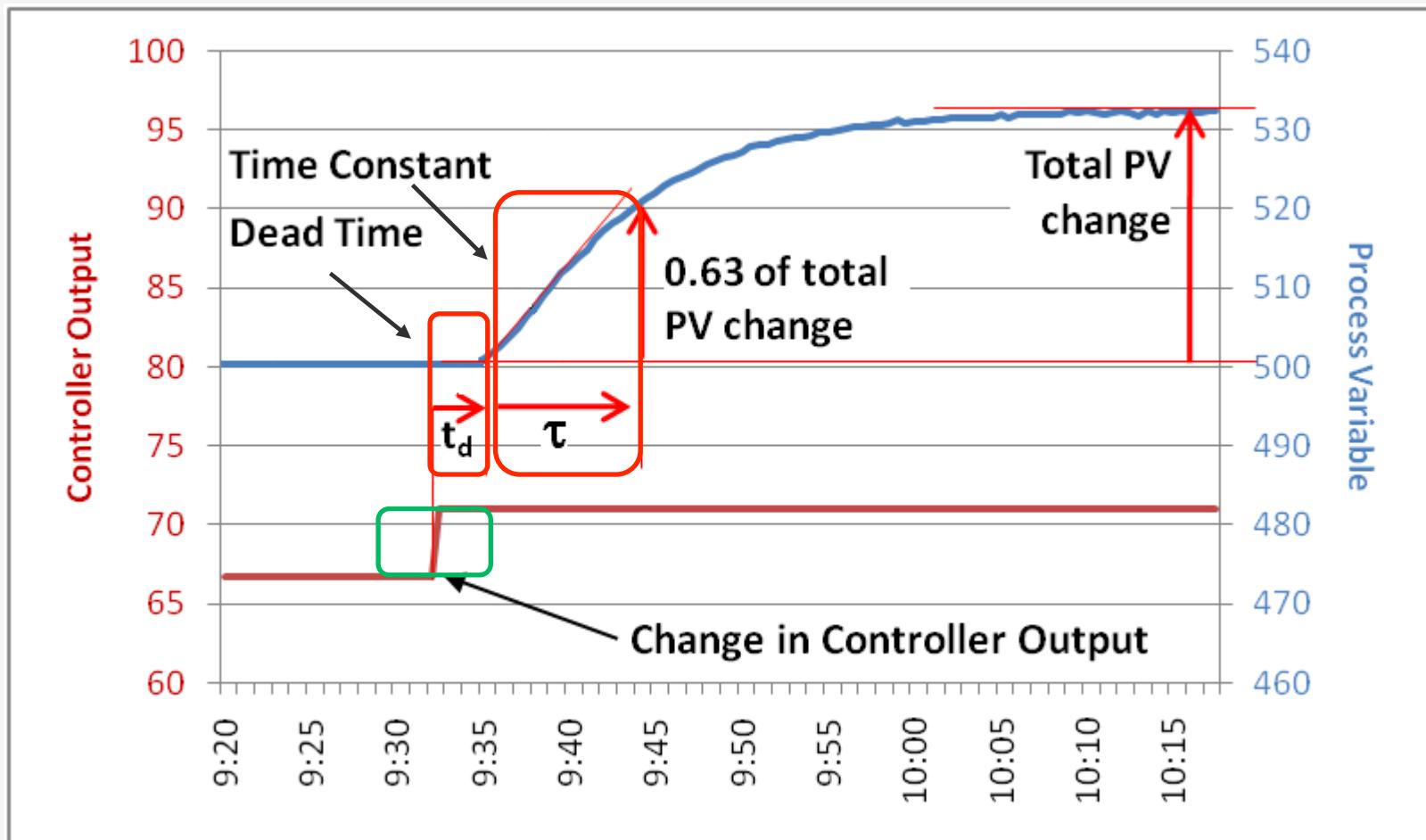
PID control



$$u(t) = K \left(e(t) + \frac{1}{T_i} \int_0^t e(\tau) d\tau + T_d \frac{de(t)}{dt} \right)$$

- **PID: proportional, integral, derivative** – most widely used control algorithm on the planet
- The sum of 3 components makes the final control signal
- PI controllers are most often used

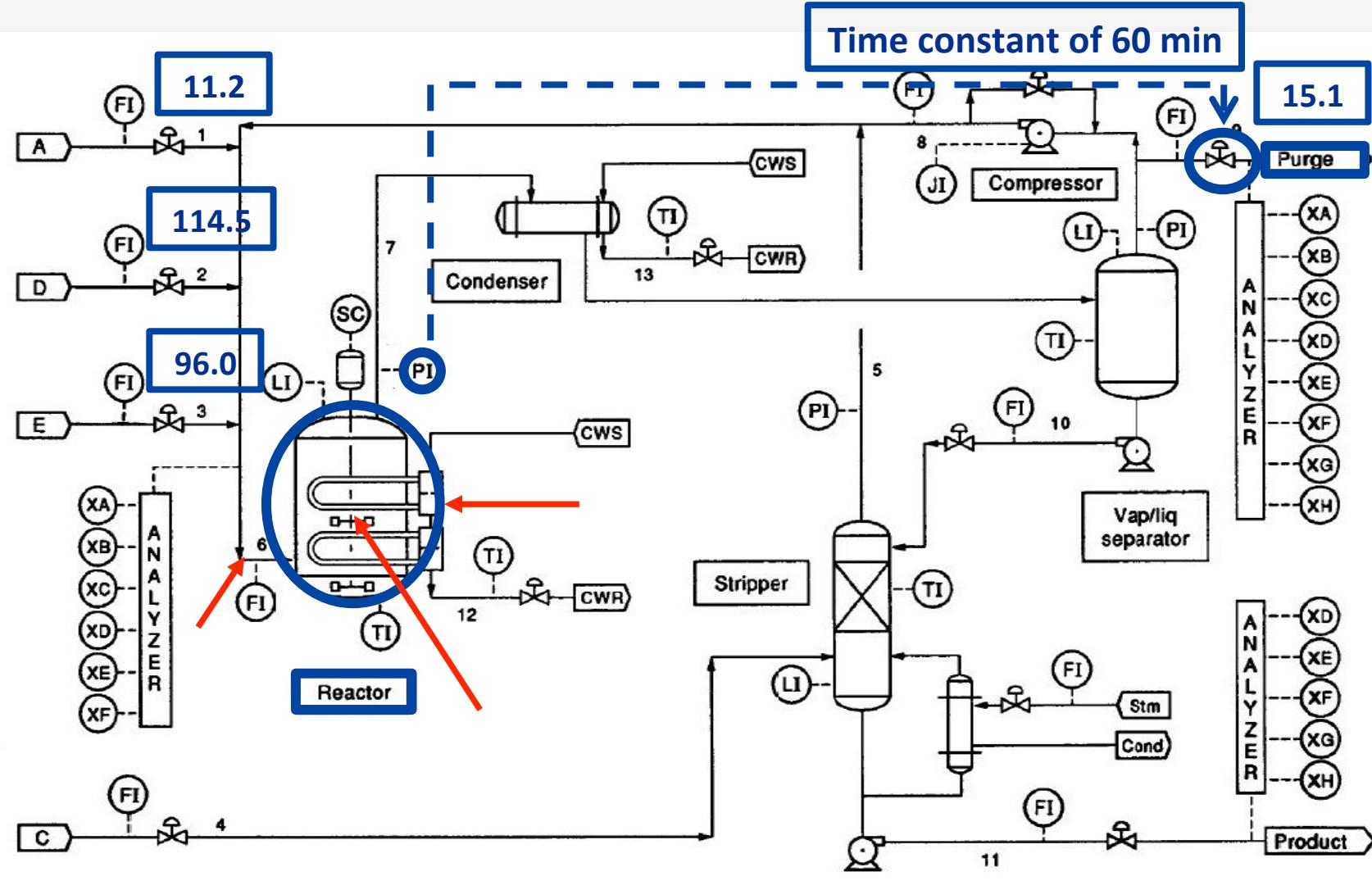
Time constants



Requires reconnaissance on live process

Jacques Smuts „Process Control for Practitioners“

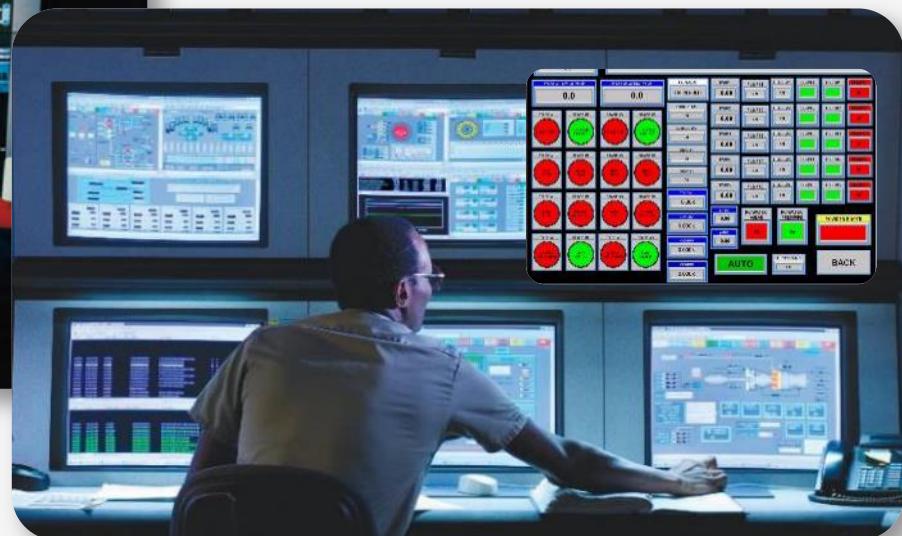
Process control vulnerability



PLC cannot do it alone



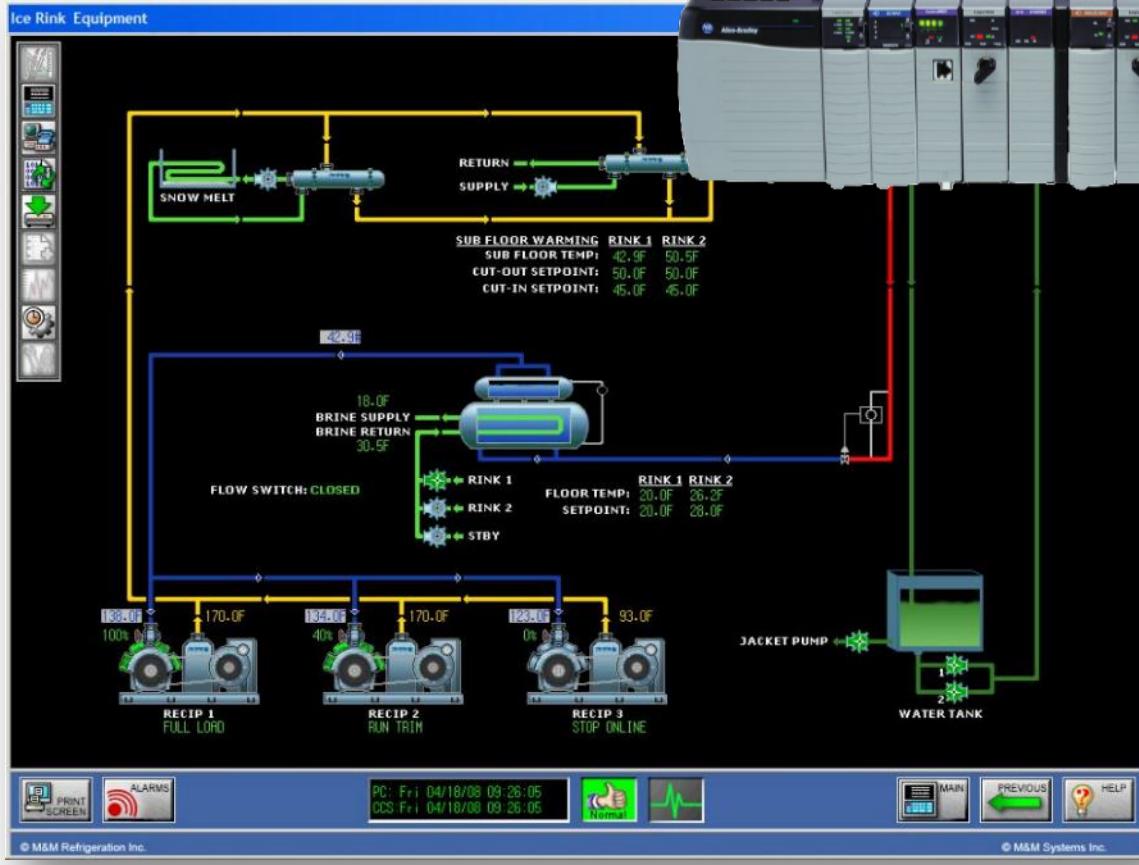
- PLC does not have the complete picture and time trends
- Human operators watch the process 7/24
- **Most important task: resolving of alarms**



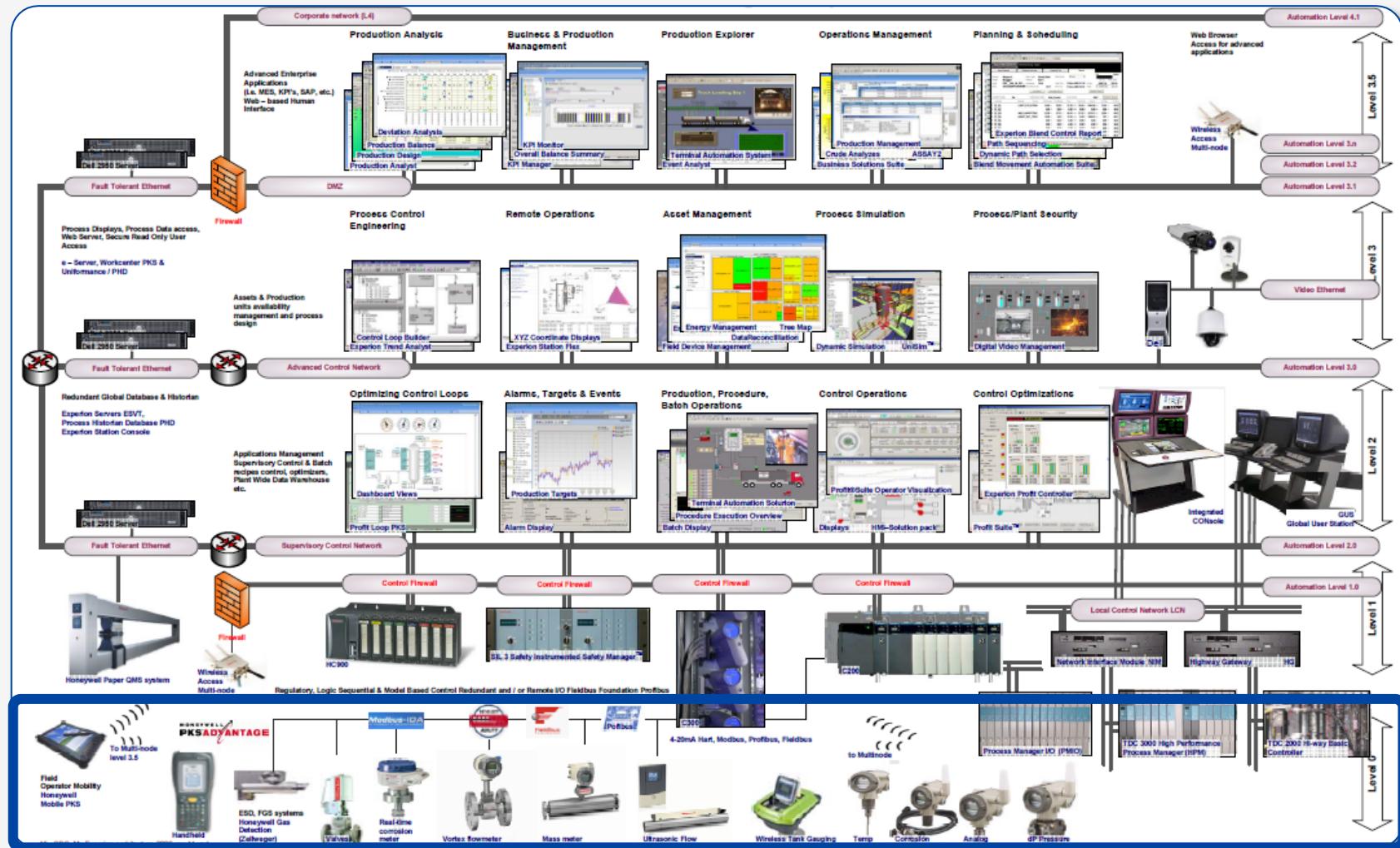
Operator is not almighty



Sanity checks



Industrial Control Systems aka SCADA



Definition of real time (time constant)

Physical process



Why to hack SCADA

Industrial Control Systems



**Industry means big business
Big business == \$\$\$\$\$\$**



Why to attack ICS



**Industry means big business
Big business ==\$\$\$\$\$**

Alan Paller of SANS (2008):

In the past two years, hackers have successfully penetrated and extorted multiple utility companies that use SCADA systems.

Hundreds of millions of dollars have been extorted, and possibly more. It's difficult to know, because they pay to keep it a secret.

This kind of extortion is the biggest untold story of the cybercrime industry.

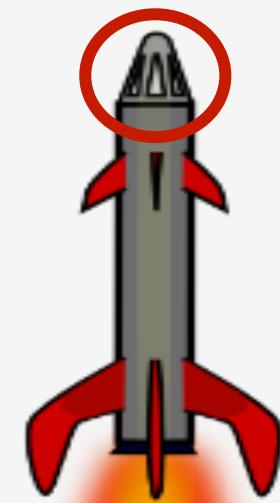
Attack payload



Attack
objective



Cyber-physical
payload



What can be done to the process



Equipment damage

- Equipment overstress
- Violation of safety limits

Production damage

- Product quality and product rate
- Operating costs
- Maintenance efforts

Compliance violation

- Safety
- Pollution
- Contractual agreements

Paracetamol



Purity	Relative price, EUR/kg
98%	1
99%	5
100%	8205

Source: <http://www.sigmaaldrich.com/>



Attack considerations



Equipment damage

- Comes first into anybody's mind (+)
- Irreversible (±)
- Unclear collateral damage (-)
- May transform into compliance violation, e.g. if it kills human (-)

Equipment damage

Production damage

Compliance violation

Compliance violation

- Must be reported to the authorities (±)
- Will be investigated by the responsible agencies (-)
- Compliance regulations are public knowledge (+)
- Unclear collateral damage (-)

Production damage attack



Attack goal: persistent economic damage



Get the party started!

Plants for sale



From LinkedIn



+Follow Tommy

Used VAM - Vinyl Acetate Monomer plant for sale & relocation! If any interest, please contact me!

Tommy Heino

Industrialist & Entrepreneur, Owner, XHL Business Engineering
Top Contributor

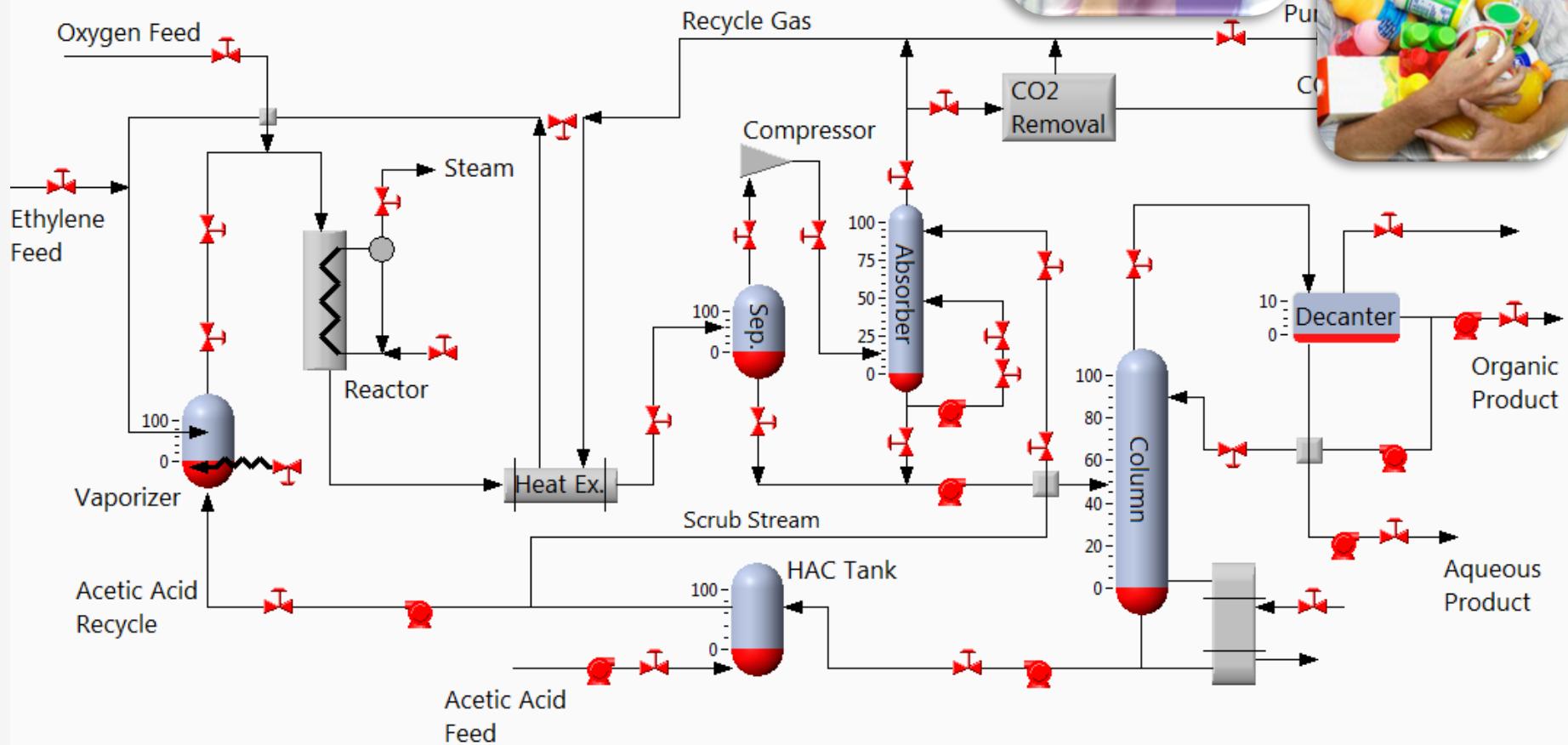
Like • Comment (4) • Share • Follow • 3 months ago



More plants offers:

<http://www.usedplants.com/>

Vinyl Acetate Monomer plant (model)



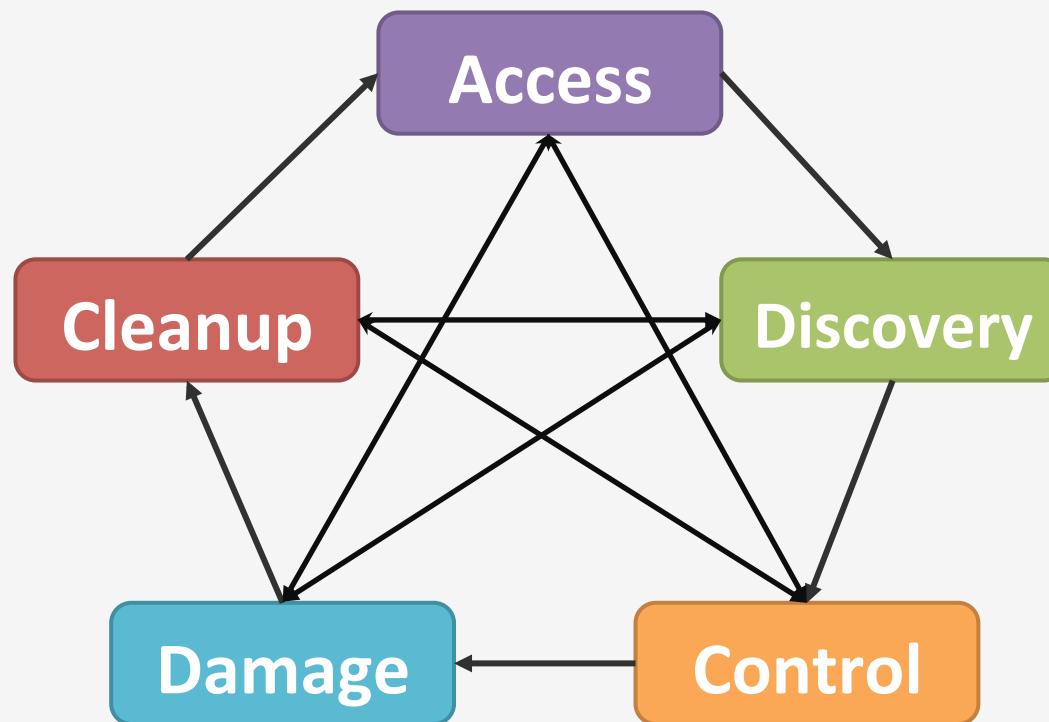


Stages of cyber-physical attacks

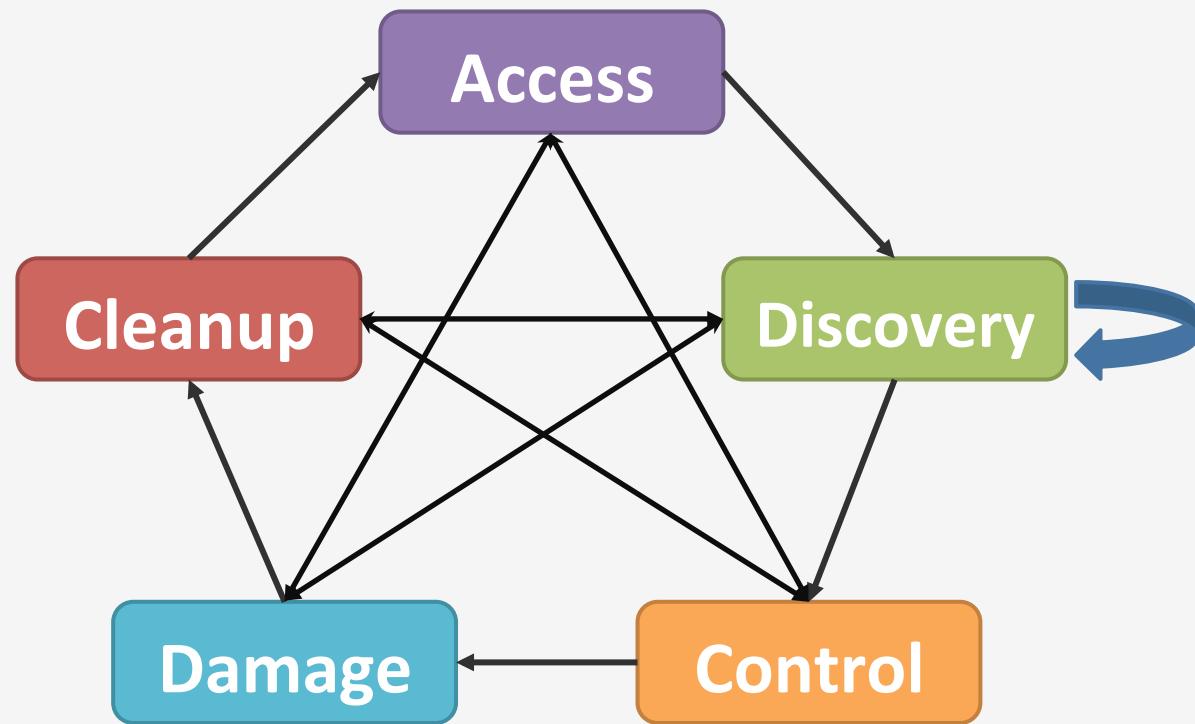
Hacking Chemical Plant for Competition & Extortion



Stages of SCADA attack



Stages of SCADA attack





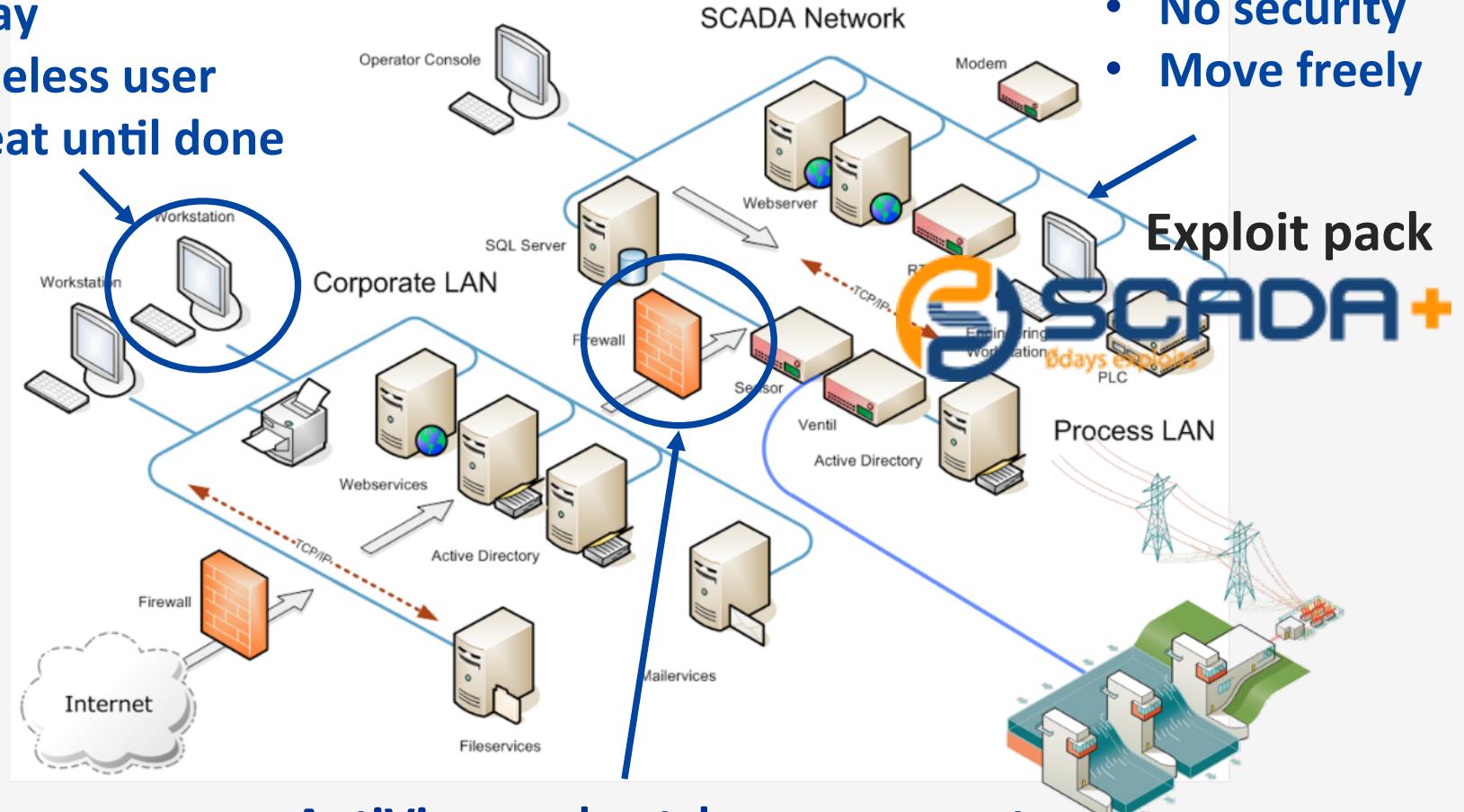
Access



Traditional IT hacking



- 1 Oday
 - 1 Clueless user
 - Repeat until done



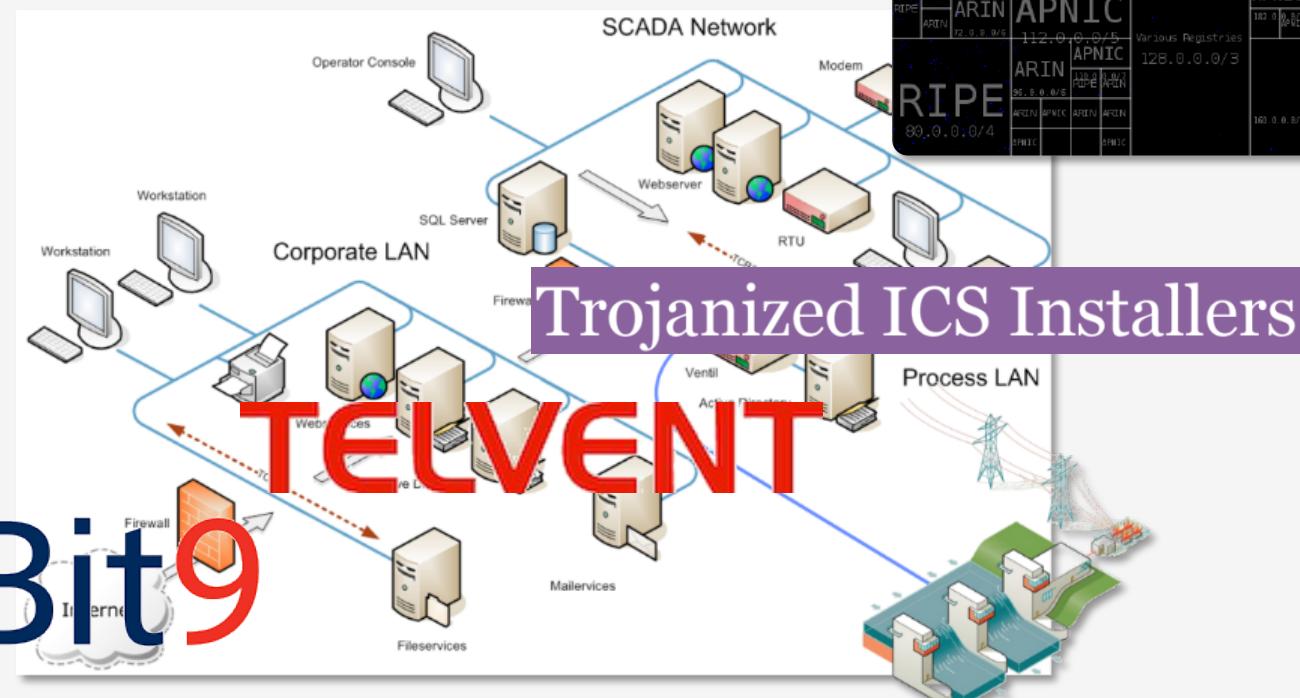
- AntiVirus and patch management
 - Database links
 - Backup systems

Modern IT hacking



- Select a vulnerability from the list of ICS-CERT advisories
- Scan Internet to locate vulnerable devices
- Exploit

GE		HP		DEC		Multicast		Reserved	
RIPE	APNIC	AT&T	NTT	MIT	ARIN	DISA			
RIPE	APNIC	IBM	AT&T	MIT	ARIN	DISA			
APNIC	AT&T	NTT	APNIC	RIPE	APNIC	DISA			
APNIC	AT&T	NTT	APNIC	RIPE	APNIC	DISA			
APNIC	224.0.0.0/4								
APNIC	220.0.0.0/6								
APNIC	212.0.0.0/7								
APNIC	204.0.0.0/7								
APNIC	196.0.0.0/7								
APNIC	188.0.0.0/7								
APNIC	180.0.0.0/7								
APNIC	172.0.0.0/7								
APNIC	164.0.0.0/7								
APNIC	156.0.0.0/7								
APNIC	148.0.0.0/7								
APNIC	140.0.0.0/7								
APNIC	132.0.0.0/7								
APNIC	124.0.0.0/7								
APNIC	116.0.0.0/7								
APNIC	108.0.0.0/7								
APNIC	100.0.0.0/7								
APNIC	92.0.0.0/7								
APNIC	84.0.0.0/7								
APNIC	76.0.0.0/7								
APNIC	68.0.0.0/7								
APNIC	60.0.0.0/7								
APNIC	52.0.0.0/7								
APNIC	44.0.0.0/7								
APNIC	36.0.0.0/7								
APNIC	28.0.0.0/7								
APNIC	20.0.0.0/7								
APNIC	12.0.0.0/7								
APNIC	4.0.0.0/7								
APNIC	0.0.0.0/7								



- E. Leverett, R. Wightman. Vulnerability Inheritance in Programmable Logic Controllers (GreHack'13)



Discovery

Know the equipment

Stripping column aka stripper



Process discovery



What and how the process is producing



How it is controlled



How it is build and wired



Operating and safety constraints

Espionage, reconnaissance
Target plant and third parties

Espionage



- Industrial espionage has started LONG time ago
(malware samples dated as early as 2003)

Cyber Espionage comes to SCADA Security

Over Half of ICS Security Incidents Reported in 2011 Involved APTs: ICS-CERT

Nitro Malware Targeted Chemical Companies

ment, and manufacture of chemicals and advanced materials. The goal of the attackers appears to be to collect intellectual property such as design documents, formulas, and manufacturing processes

Dragonfly: Western Europe's East

Cyberespionage campaign stole info

DragonFly/Havex/Energetic Bear Malware

ACAD/Medre.A 10000's of AutoCAD files leaked in suspected industrial espionage

BY RICHARD ZWIEBEL June 25, 2014

"VIRUSES REVEALED"

Nation state behind malware attacks on European ICS systems?

Process discovery

1.

$$\text{H}_3\text{C}-\overset{\text{H}}{\underset{\text{H}_2}{\text{C}}}-\overset{\text{O}}{\underset{\text{H}_3\text{C}}{\text{C}}}-\text{H} \xrightarrow[\text{heat}]{\text{H}^+} \text{H}_3\text{C}-\overset{\text{H}}{\underset{\text{H}_2}{\text{C}}}-\overset{\text{O}}{\underset{\text{H}_3\text{C}}{\text{C}}}-\text{H} + \text{H}_3\text{O}^+$$

AVEVA Instrumentation Engineer

Instrument Datasheet
PRESSURE TRANSMITTER

Tag No.	01-PT-510
Service	Reactor 01-R-510
PNL No.	Line Number 01-220-004
Area Classification	Zone 1, Gc, IC, T3
Process Protection	

PROCESS CONDITIONS

Fluid	State	HCl	Viscosity	Design Pressure	Min-Max	Max	Design Temperature	Min-Max	Max
Pressure	Normal Max	1200 kPa		1430 kPa	-/-	1590 kPa	Temperature	Normal Max	149 °C
Temperature	Normal Max	100 °C		149 °C	-/-	148 °C			

Loop番号: 01-T-511 ループサービス: Reactor 01-R-510

ループ番号: 01-JB-002

AVEVA Instrumentation カタログレポート

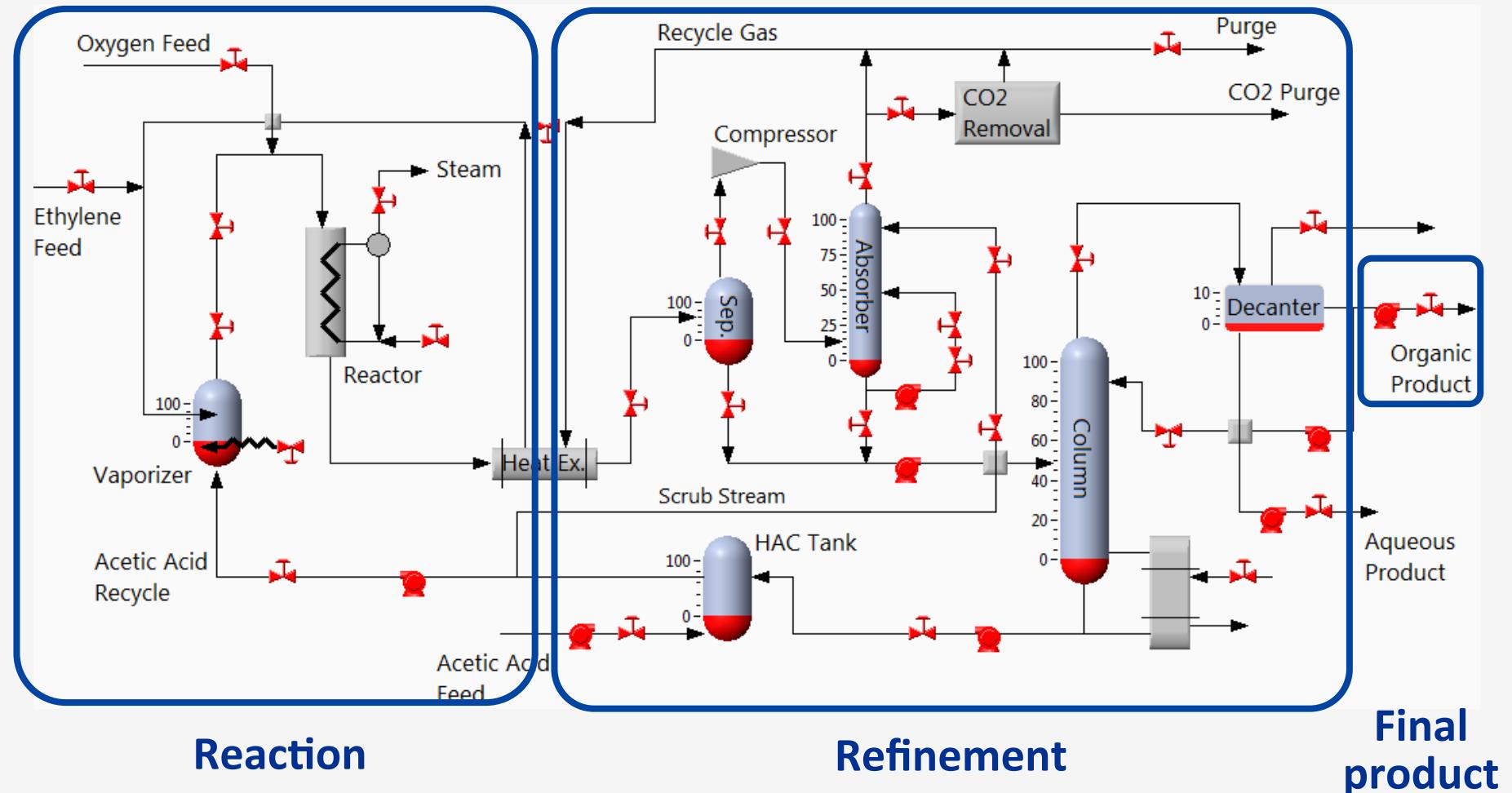
01-TT-511	01-JB-002
01-FT-510	01-JB-002
01-LV-525	01-JB-002
01-LS-525	01-JB-002
01-PT-500	01-JB-002
01-FE-520	01-JB-002
01-FT-520	01-JB-002
01-FE-600	01-JB-002
01-FV-600	01-JB-002
01-FT-003	01-JB-002
01-FALL-510	01-JB-002
01-LG-526	01-JB-002
01-PI-527	01-JB-002

Table of Contents

- Generator
- Grader
- Man Basket
- Other
- Plow
- Pressure Vessel
- Pump
- Quad
- Rig Mats
- Shacks
- Threader
- Tractor
- Trailer

14	DS-01	DblShift 01	DSHIFT	20 Ton Picker	1D7HU18278S618229
15	E100	E100 336DL	Galaxy	Excavator	1GCHK29141E302402
16	E101	E101 325D	Galaxy	Excavator	5TFHY5F1XAX097175
17	E102	E102 325BL	Galaxy	Excavator	1D7RV1CT2AS149221
18	E103	E103 320CL	Galaxy	Excavator	3D7UT2HL5AG134976
19	E104	E104 320CL	Galaxy	Excavator	
20	Enclosed Trailer	Enclosed Trailer	PR SERVICES	Trailer	
21	FS 08	Flare Stack 08	Galaxy	Other	
22	FSH 1	Flameless Space Heater	PR SERVICES	Other	
23	G100	G100	Galaxy	Grader	
24	G101	G101	Galaxy	Grader	
25	G103	G103	Galaxy	Grader	
26	Gas Monitor	Gas Monitor	PR SERVICES	Other	
27	Generator	Generator	PR SERVICES	Generator	

Max economic damage?



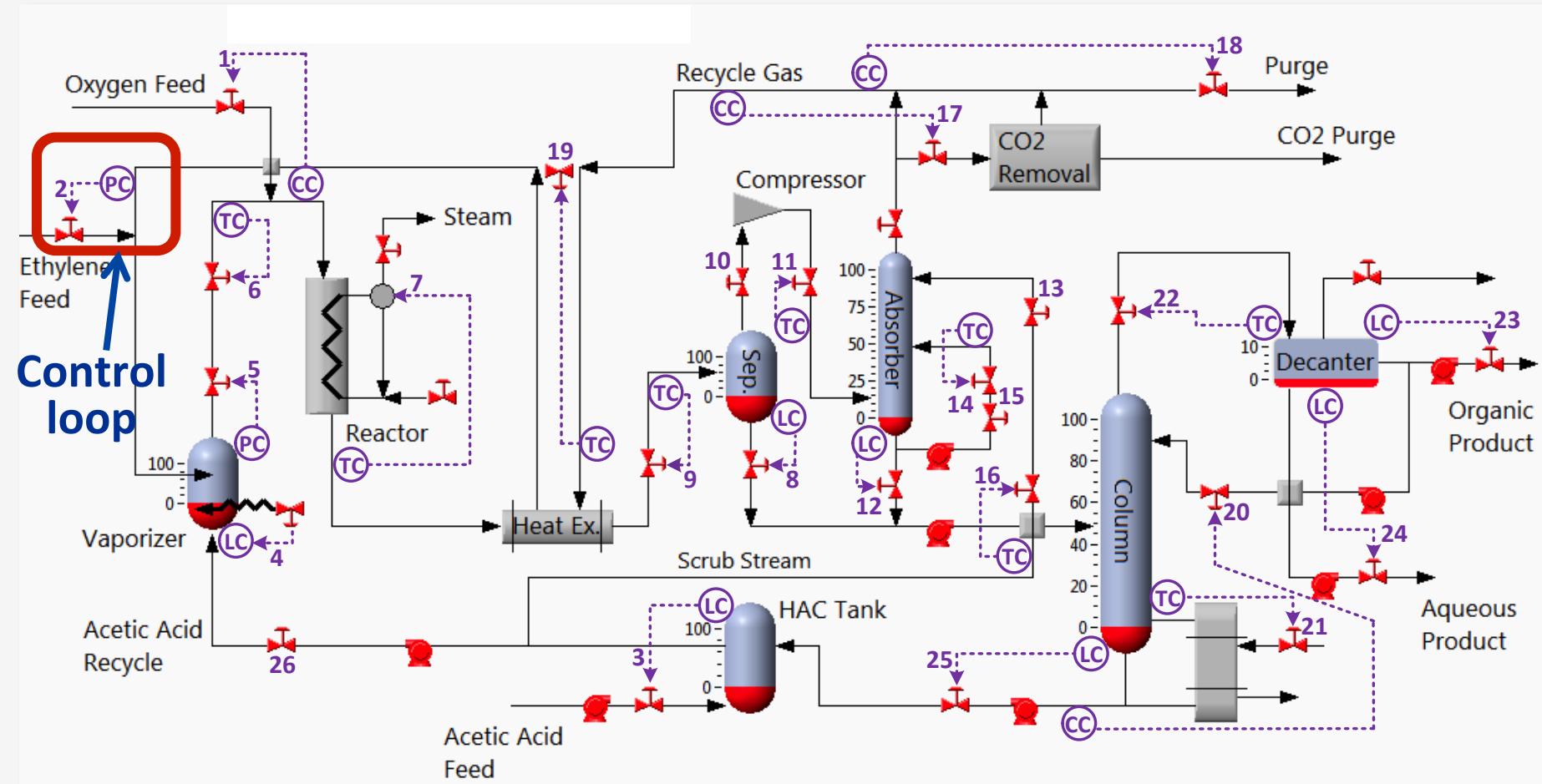
Reaction

Refinement

Final
product

Requires input of subject matter experts

Understanding control structure



Control loop configuration

AVEVA Instrumentation Engineer Contextual Action...

Project Home Data Management View Instruments

Database Audit Revisions Log Claims Publish to AVEVA NET AVEVA Tags Import AVEVA Integration

From Excel I/O Allocations Export to Excel From Other Project Attached Documents Import Export to PDF Export to XPS

Instruments

Drag a column header here to group by that column.

Area	Tag No.	Loop No.	Loop Service	Loc	Status	Description	Instrument Service	Manufacturer	Model No.	Assoc Equip	Size	P/I D No.	Data Sheet No.	Loop Dwg No.	General Hook	Pro
01	01-FT-003	01-F-003		FLD	New	D/P Transmitter										
01	01-AE-100			FLD		Sulphur Analyser										
01	01-PT-500	01-P-500	Feed Surge Drum 01-V-500	FLD	Existing	Transmitter	Feed Surge Drum 01-V-500	Yokogawa	EJA110A	01-V-500	01-220-004	700001-2	01-P-500			
01	01-PT-510	01-P-510	Reactor 01-R-510	FLD	New	Transmitter	Reactor 01-R-510	Yokogawa	EJA110A	01-P007-80-B1	01-220-004	700001-1				
01	01-FE-510			FLD	Existing	Orifice Plate	Reactor 01-R-510 Feed									
01	01-FT-510	01-F-510	Reactor 01-R-510 Feed	FLD	Replace	D/P Transmitter	Reactor 01-R-510 Feed									
01	01-FC-510	01-F-510	Reactor 01-R-510 Feed	DCS	New	Controller	Reactor 01-R-510 Feed									
01	01-FAL-510	01-F-510	Reactor 01-R-510 Feed	DCS	New	Alarm Low	Reactor 01-R-510 Feed									

700001-1

Save Copy Print Preview Issue Reset Zoom Preferences Default Project Process Units : Density: kg/m³ Flow: kg/hr Level: mm Mass: kg Pressure: bar Temperature: °C Viscosity: mPa.s

DSS2040

Instrument Datasheet

PRESSURE TRANSMITTER

1 Tag No.	01-PT-510			
2 Service	Reactor 01-R-510			
3 P&ID No:	Line Number	01-220-004	01-P007-80-B1	
4 Area Classification	Zone 1, G1IIC, T3			
5 Ingress Protection	IP 67			
PROCESS CONDITIONS				
7 Fluid	State	HC	Vapour	
8 Pressure	Normal	Max	1450 KPag	1650 KPag
9 Temperature	Normal	Max	100 °C	149 °C
				Design Pressure Min/Max
				Design Temperature Min/Max
TRANSMITTER				
11 Instrument Range	LRV / URV / Un	-0.5	14	MPa
12 Calibration Range	LRV / URV / Un	0	1700	KPag
13 Accuracy	+/- 0.075% of Span			Downscale
14 Elevation	Suppression	-	-	Installation Style
15 LP Proc. Conn.	HP Proc. Conn.	1/4" NPT-F	Vent to Atmosphere	Horizontal Impulse
16 Conduit Connected	Power Supply	2x M20 Female, one Blind Fl	Nominal 24VDC IS	Mounting
17 Housing	Paint	Low Copper/Cast-Aluminum A	Epoxy Resin-Baked Coating	Via Manifold Use
18				See Note 6.
ELEMENT				
20 Element Type	Element Material	DP Capsule	SUS316L	Temperature Limits Min/Max -40 °C
21 Measurement (Gauge / Abs / Vac etc)	Gauge			Pressure Limits Min/Max -
22 Body Material	Body Rating	SCS14A	16 MPa	
23 Bolts	Seals	SUS630	Teflon Coated SUS316	
24 Other wetted materials	Diaphragm-Hastelloy-C276, Vent Plug - SUS316			
25 Fill Fluid	Silicone Oil			
26 NACE Certification	MR-0175:2001 Required			
27	DIAPHRAGM SEAL			

Ready

AVEVADefault (27 Records)

Project : AI Demo SP1 User : Keith.Hiller

Audit Manager

Tools

Find Print Refresh Close

AVEVA Application Object Type

Loop List Process Data Process Equipment List Process Line List

Apply Date/Time Occurred After : 14/05/2013 00:00 Max Limit to Display : 1000

Occurred Before : 15/05/2013 00:00

Apply

Datasheet Data, Instrument List, Process Data

Drag a column header here to group by that column.

Type	Item Tag	Description	New Value	Old Value	User	TimeStamp
Datasheet Data	01-PT-510	Transmitter Upda	Downscale	Fail High = 21.6	AVEVA\keith.hiller	5/05/2013 09:5
Process Data	01-PT-510	PressureMaxUpda	1650	1430	AVEVA\keith.hiller	5/05/2013 09:5
Process Data	01-PT-510	PressureMaxUnits	KPag	KPag	AVEVA\keith.hiller	15/05/2013 09:5
Process Data	01-PT-510	PressureNormalUn	KPag	KPag	AVEVA\keith.hiller	15/05/2013 09:5
Process Data	01-PT-510	PressureNormalU	1450	1200	AVEVA\keith.hiller	15/05/2013 09:5
InstrumentList		Tag Deleted	01-FT-999	01-FT-999	AVEVA\keith.hiller	15/05/2013 09:5
InstrumentList		Tag Deleted	01-FE-999	01-FE-999	AVEVA\keith.hiller	15/05/2013 09:5
InstrumentList	01-FE-510	CalcTypeID Upda	2	1	AVEVA\keith.hiller	15/04/2013 15:0
Process Data	01-FE-510	Updated			AVEVA\keith.hiller	15/04/2013 15:0
Process Data	01-FE-510	Updated			AVEVA\keith.hiller	15/04/2013 15:0
Process Data	01-FE-510	Updated			AVEVA\keith.hiller	15/04/2013 15:0
Process Data	01-FE-510	szTemperature Up	100	100	AVEVA\keith.hiller	15/04/2013 15:0
Process Data	01-FE-510	szViscosity Update	200	200	AVEVA\keith.hiller	15/04/2013 15:0
Process Data	01-FE-510	Updated			AVEVA\keith.hiller	15/04/2013 15:0
Process Data	01-FE-510	Updated			AVEVA\keith.hiller	15/04/2013 15:0
Process Data	01-FE-510	Updated			AVEVA\keith.hiller	15/04/2013 15:0

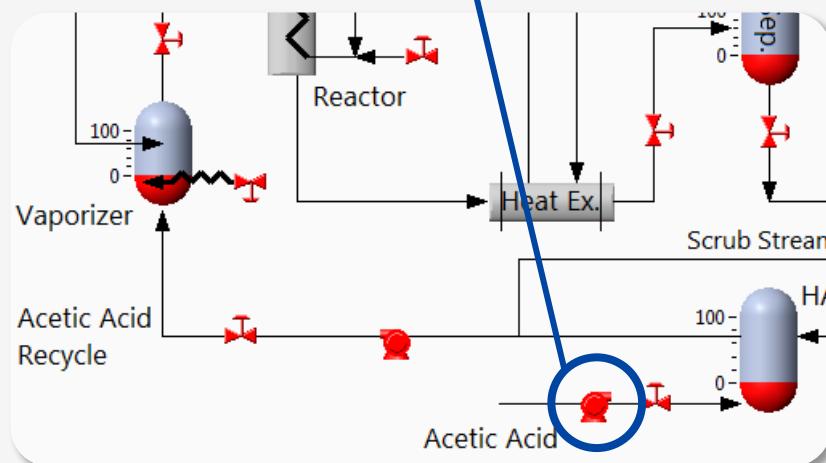
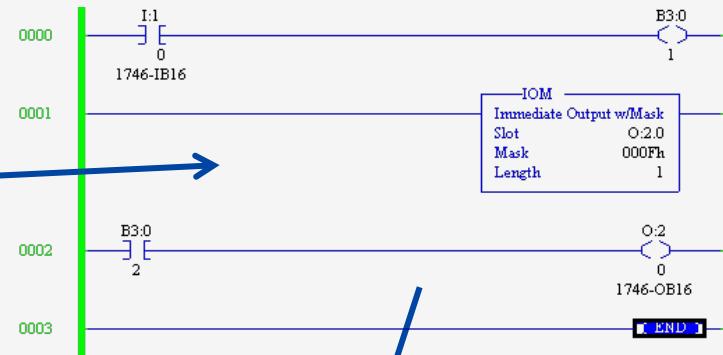
Understanding points and logic



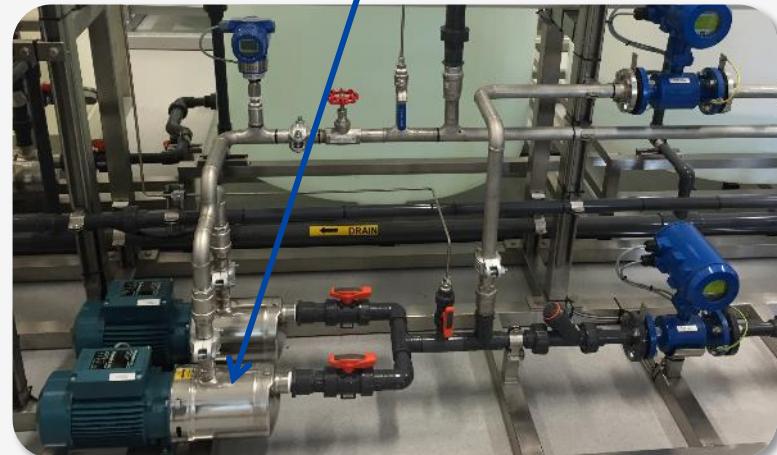
Programmable Logic Controller



Ladder logic

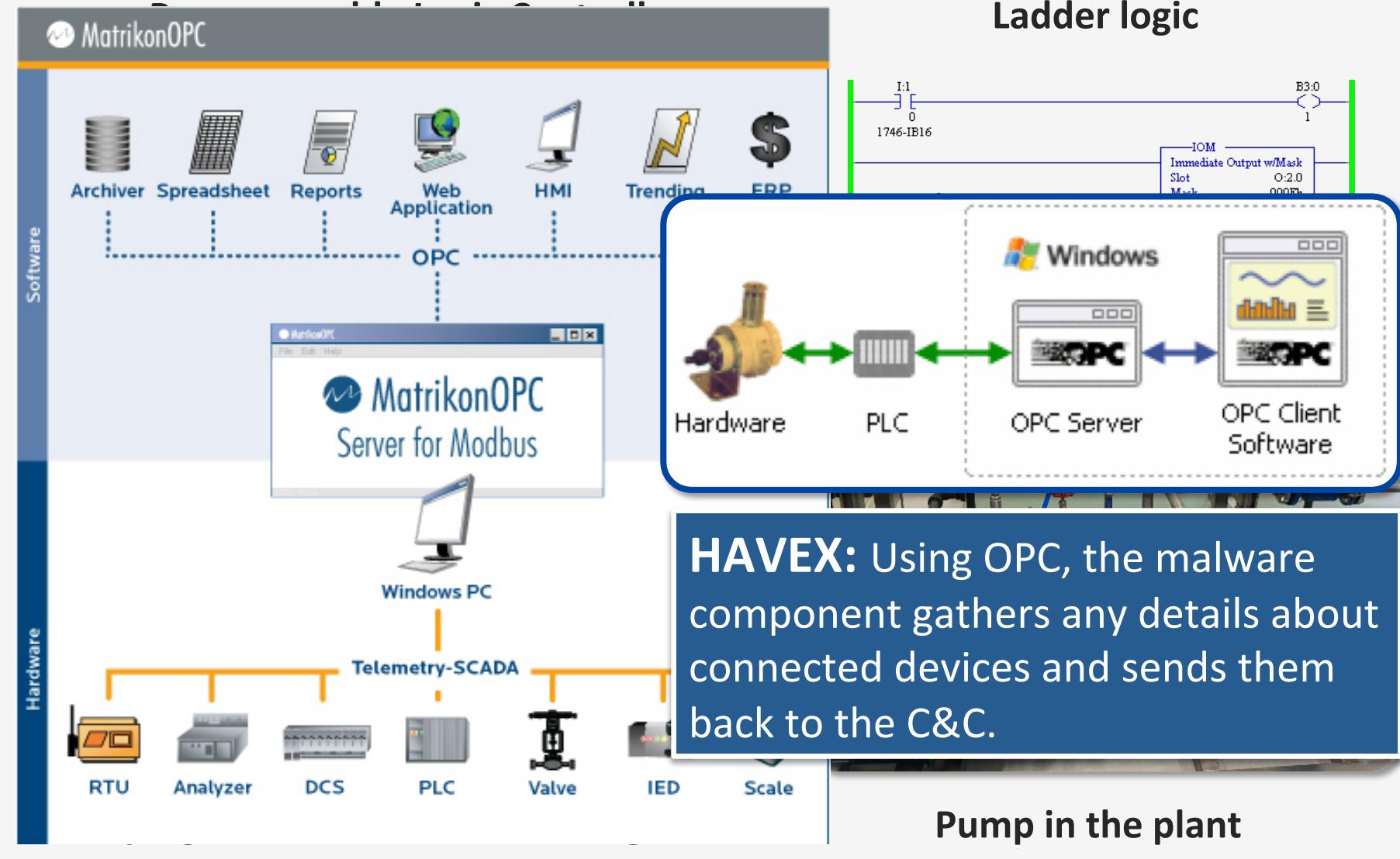


Piping and instrumentation diagram



Pump in the plant

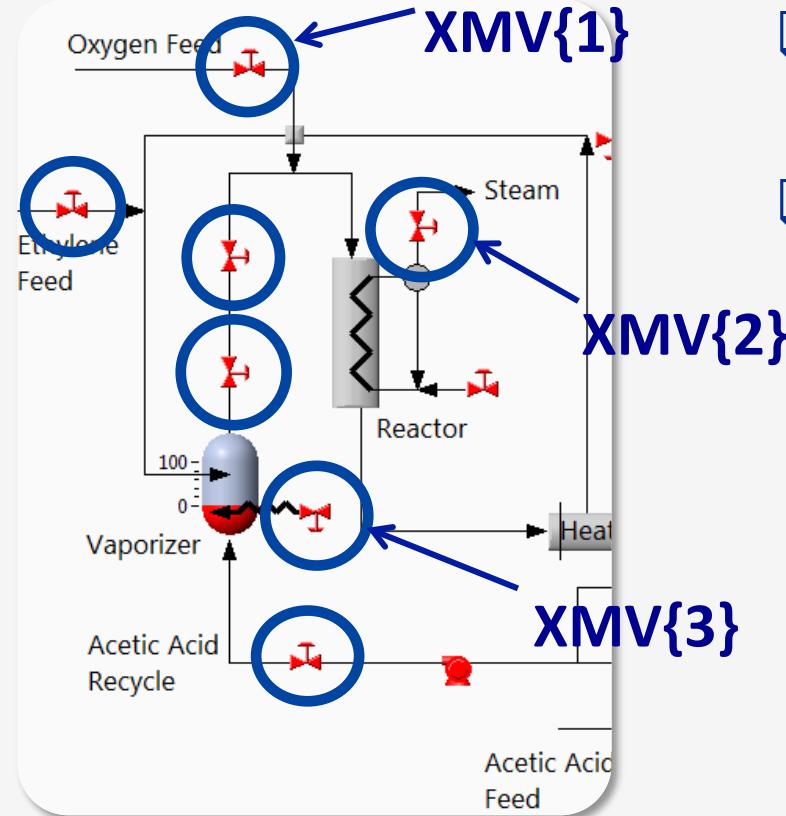
Understanding points and logic



Obtaining control != being in control



Control Loop



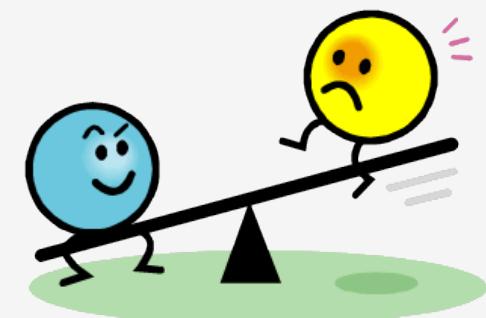
- Obtained controls might not be useful for attack goal
- Attacker might not necessarily be able to control obtained controls

???





Control



Every action has a reaction

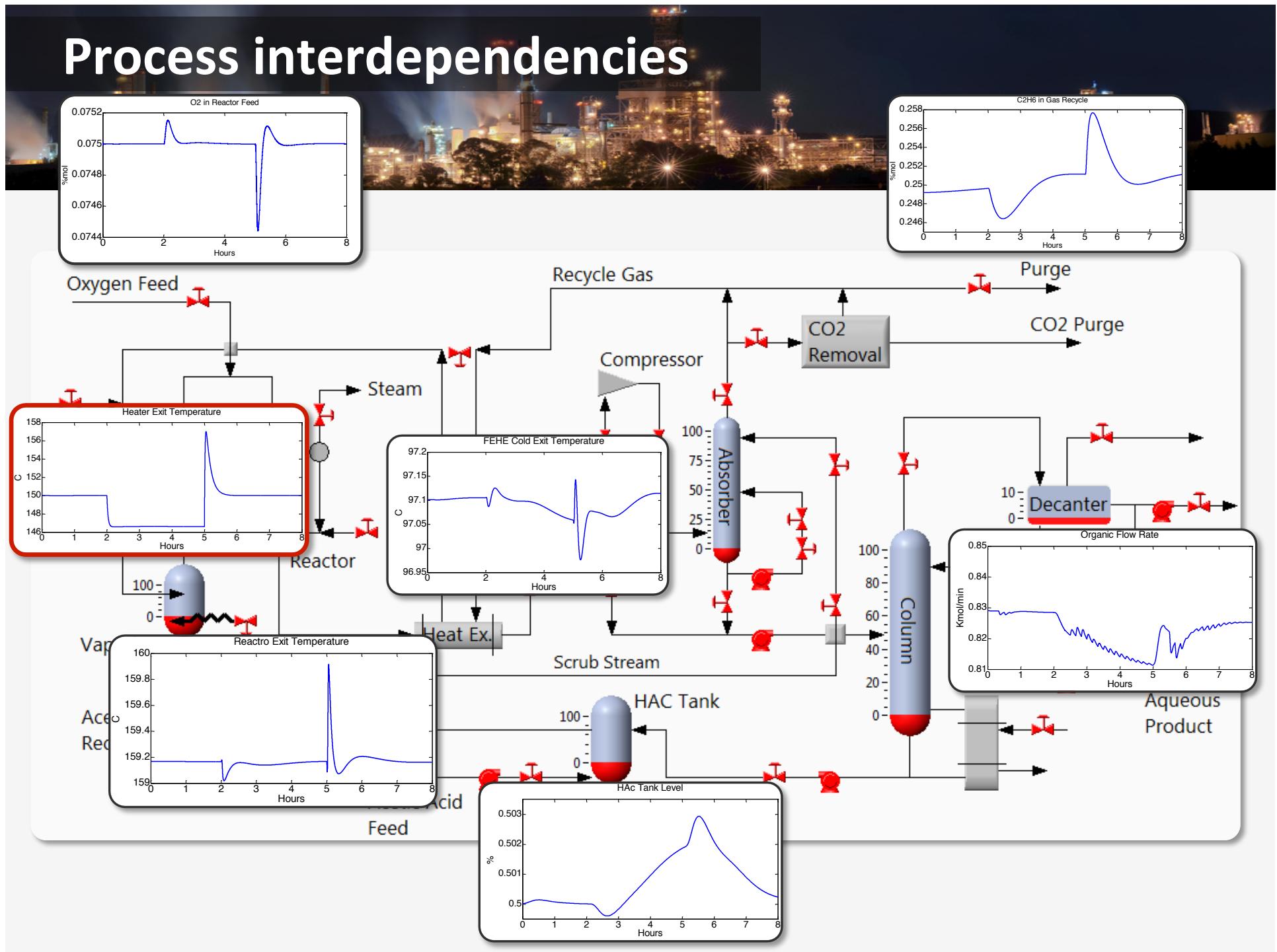
Physics of process control

Once hooked up together, physical components become related to each other by the physics of the process

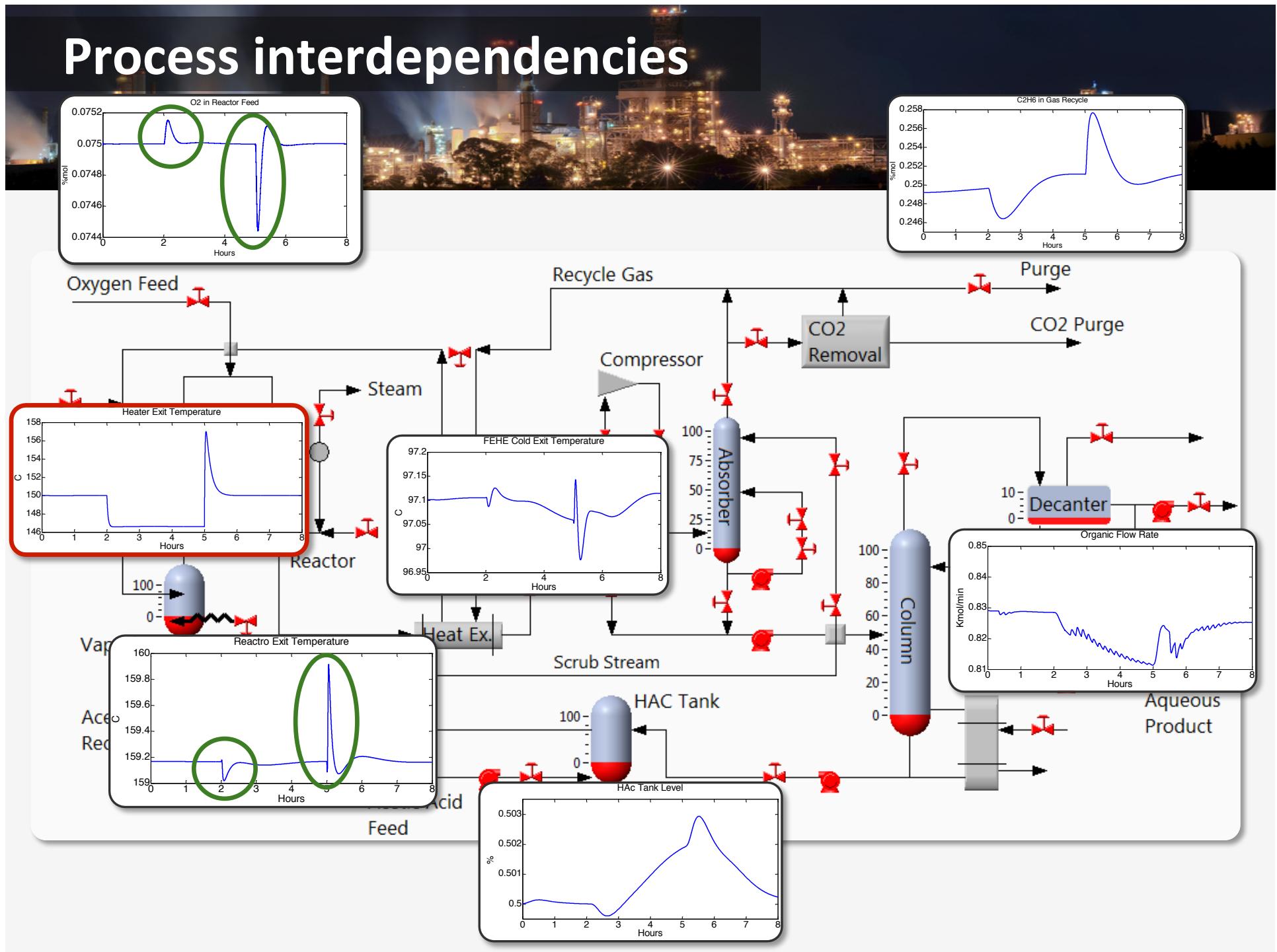


- How much does the process can be changed before releasing alarms or it shutting down?

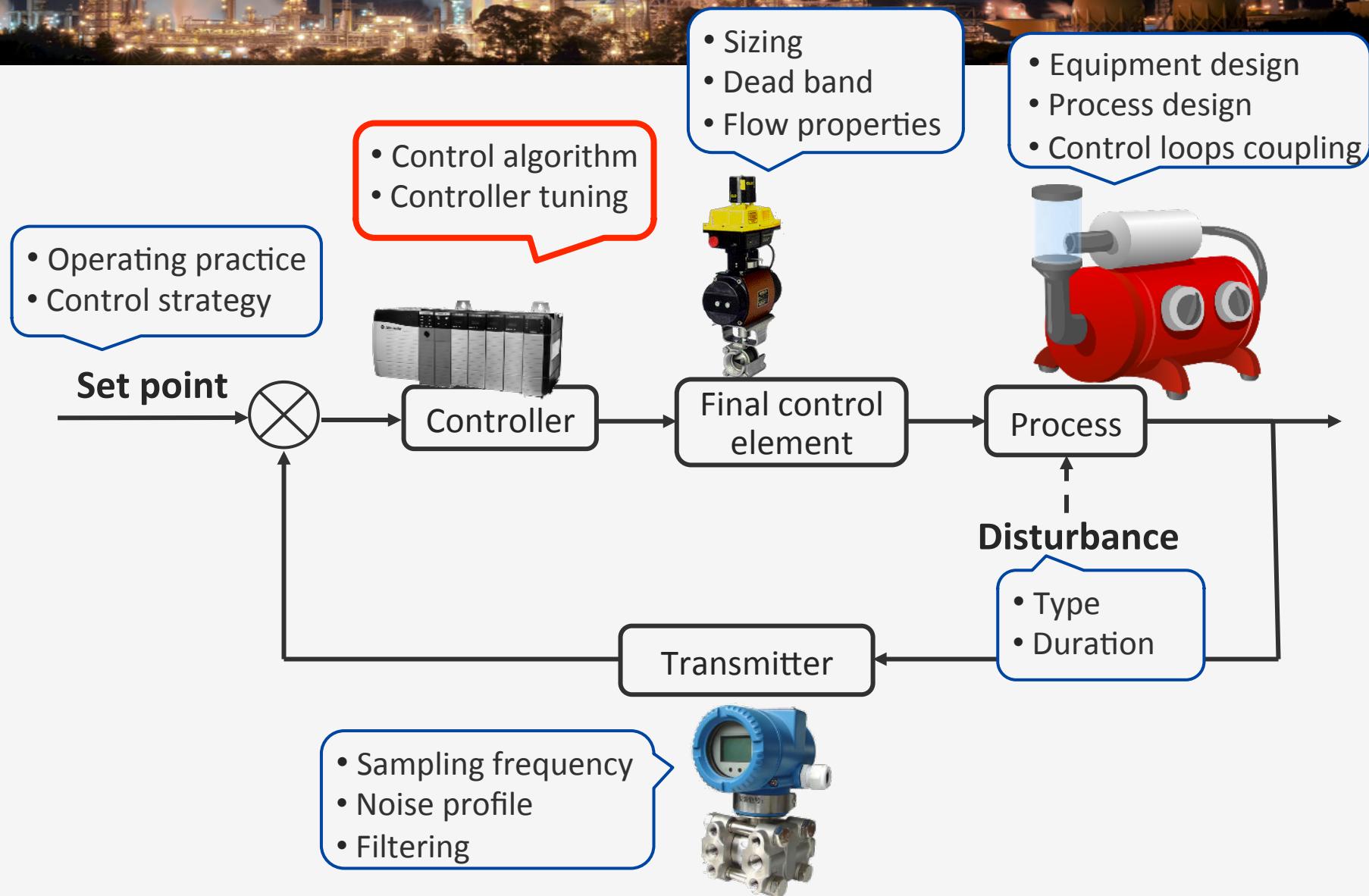
Process interdependencies



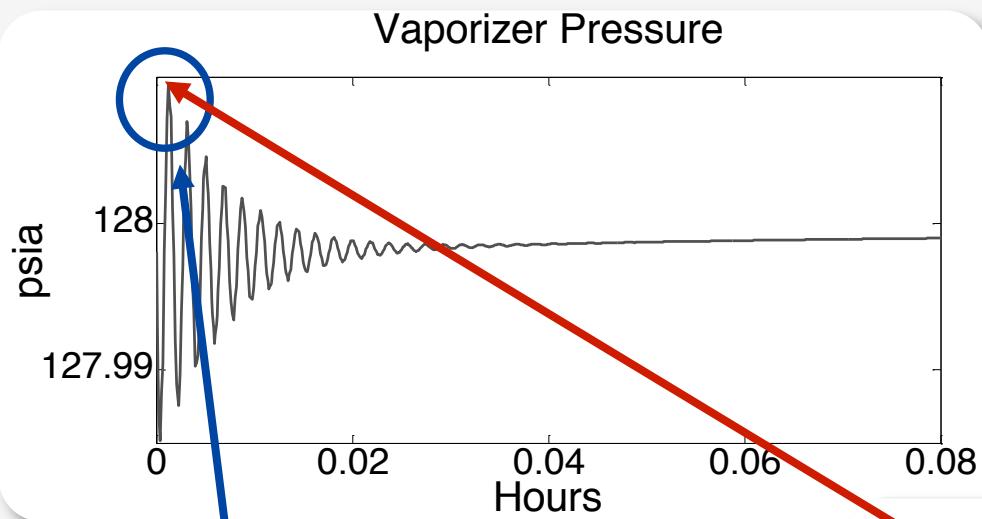
Process interdependencies



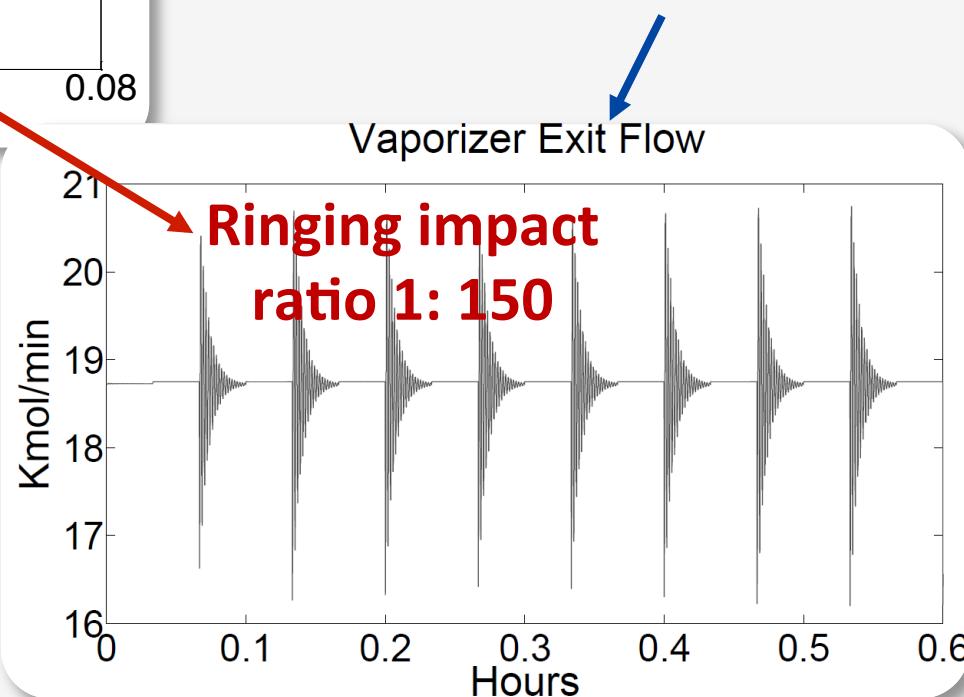
Understanding process response



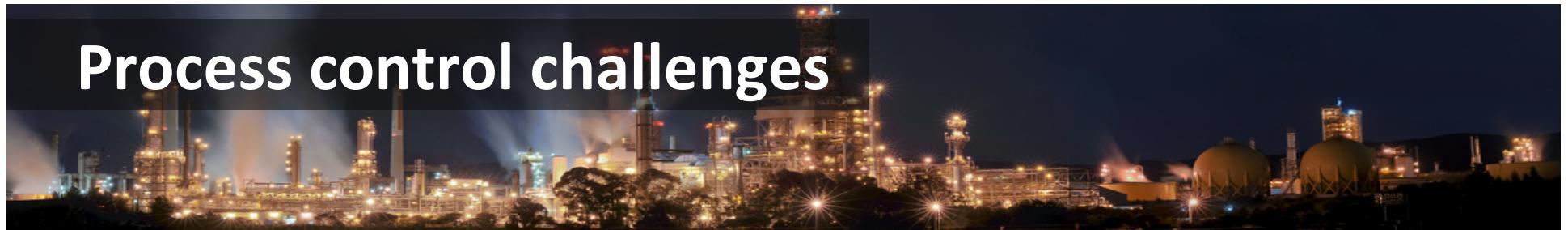
Control loop ringing



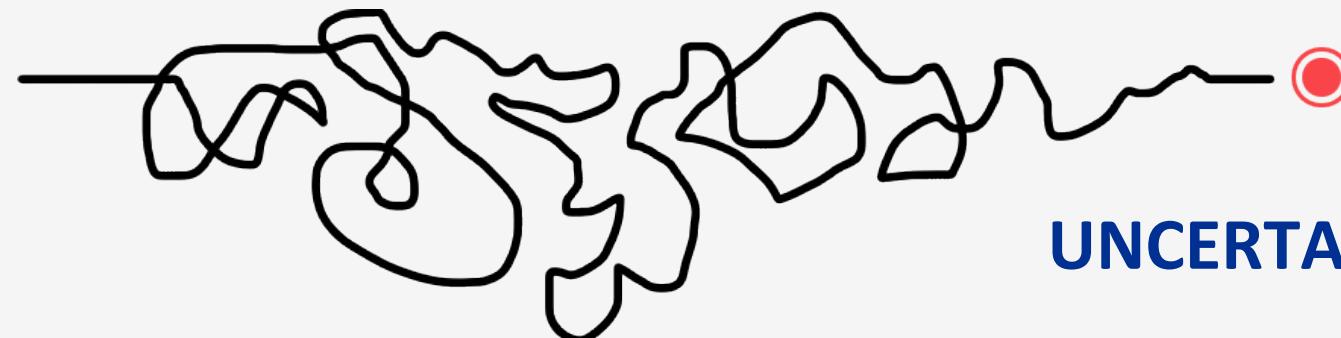
Amount of chemical entering
the reactor



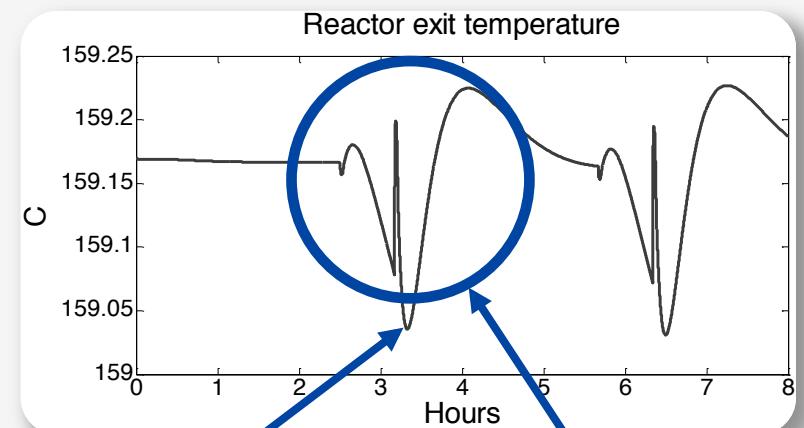
Process control challenges



- ❑ Process dynamic is highly non-linear (???)



- ❑ Behavior of the process is known to the extent of its modelling
 - So to controllers. They cannot control the process beyond their control model



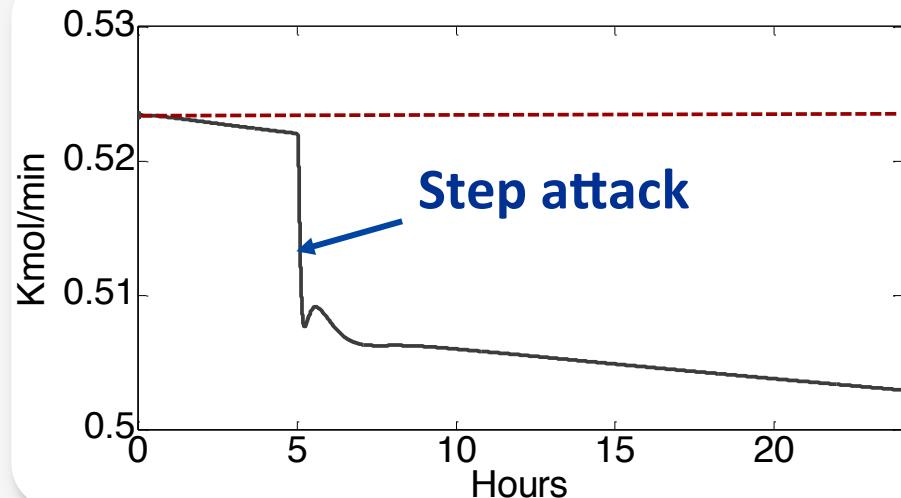
This triggers alarms

Non-linear response

Types of attacks



Fresh O₂ Feed

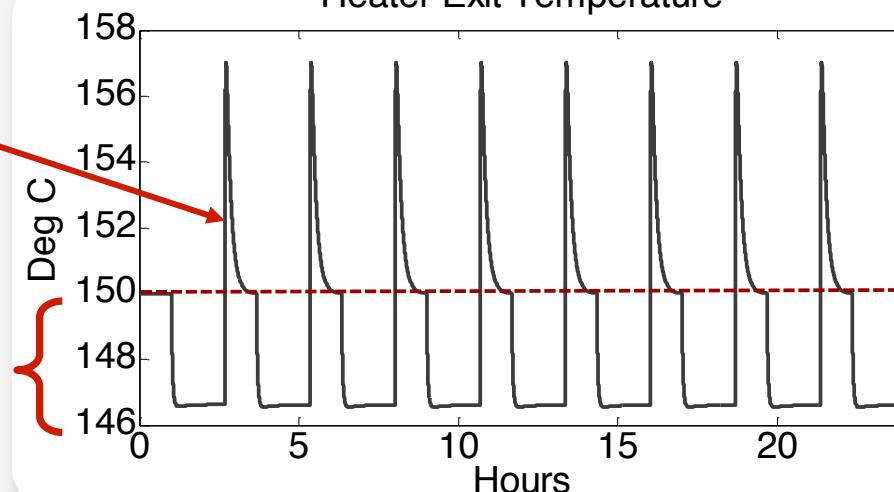


Periodic attack

Recovery time

Magnitude of manipulation

Heater Exit Temperature



Outcome of the control stage



I am 163cm tall

We should automate this process
(work in progress)



Outcome of the control stage



Sensitivity	Magnitude of manipulation	Recovery time
High	XMV {1;5;7}	XMV {4;7}
Medium	XMV {2;4;6}	XMV {5}
Low	XMV{3}	XMV {1;2;3;6}

Reliably useful controls

Alarm propagation

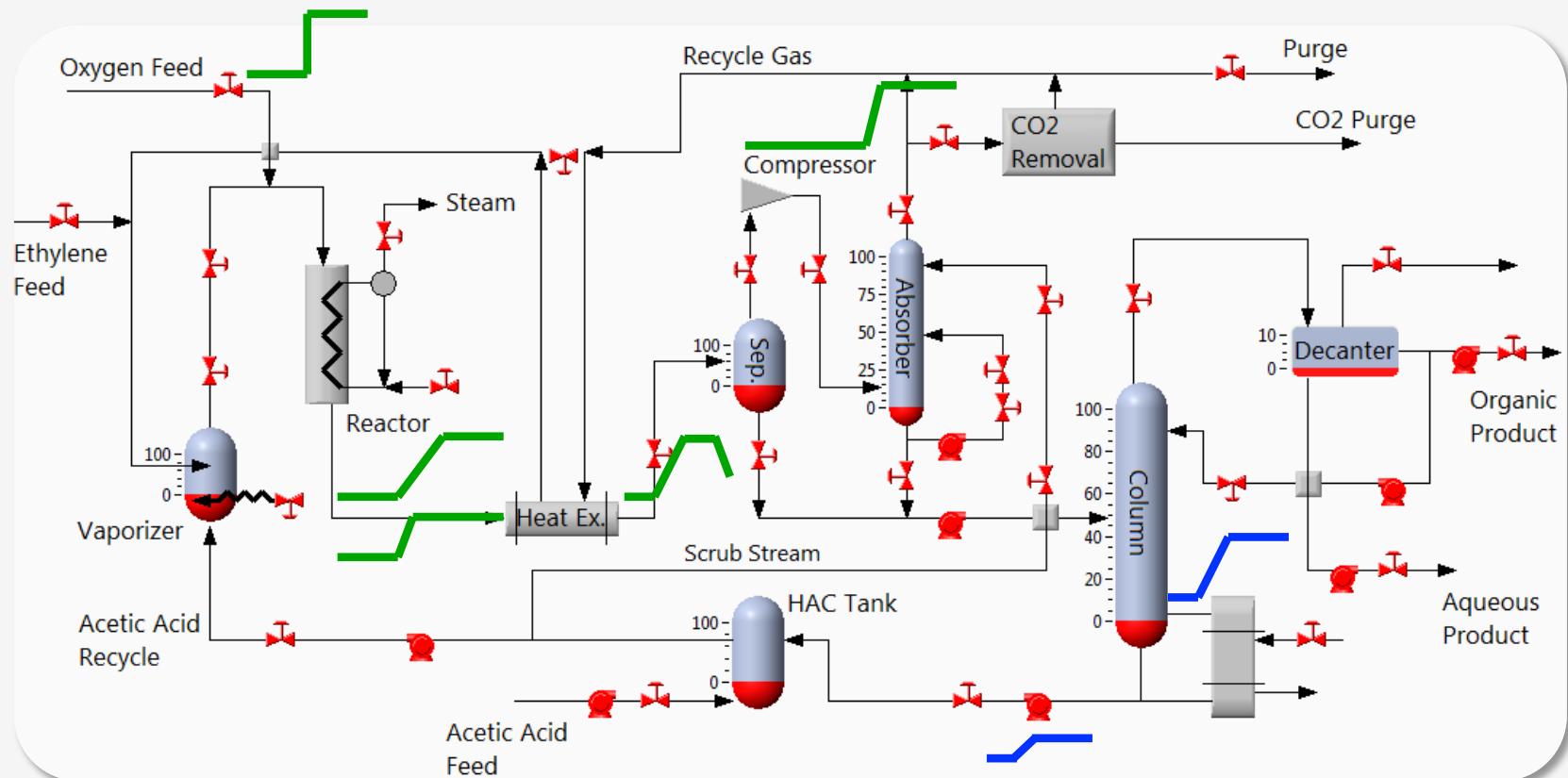


To persist we shall not bring about alarms

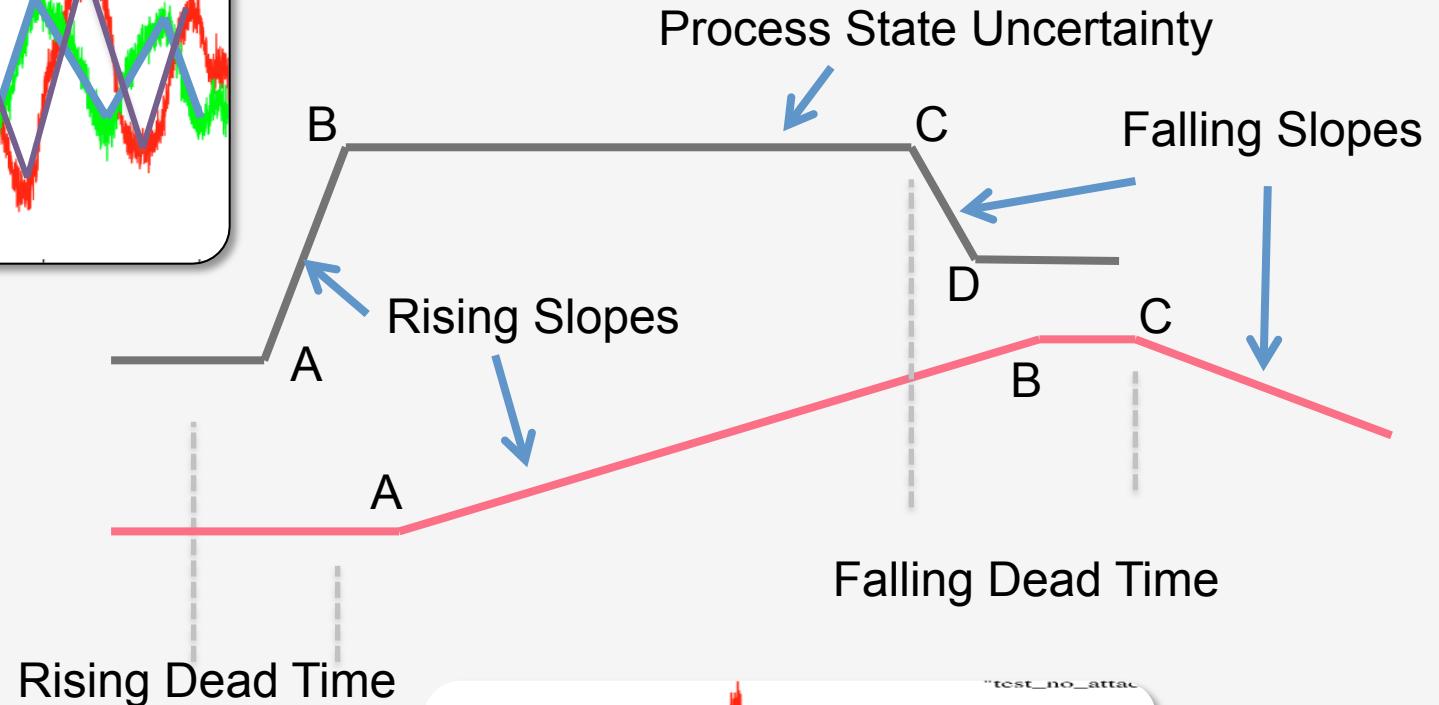
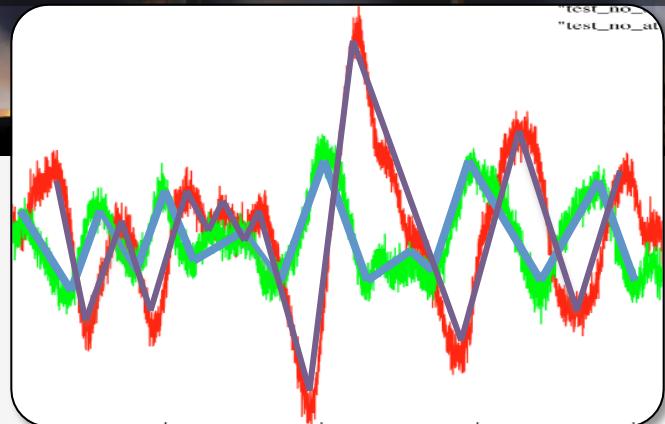
Alarm	Steady state attacks	Periodic attacks
Gas loop 02	XMV {1}	XMV {1}
Reactor feed T	XMV {6}	XMV {6}
Rector T	XMV{7}	XMV{7}
FEHE effluent	XMV{7}	XMV{7}
Gas loop P	XMV{2;3;6}	XMV{2;3;6}
HAc in decanter	XMV{2;3;7}	XMV{3}

The attacker needs to figure out the marginal attack parameters which (do not) trigger alarms

Fingerprints of plant dynamic behavior

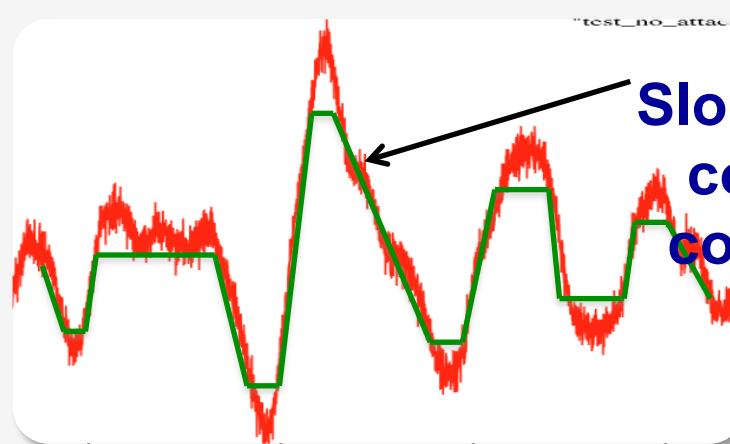


Jason Larsen at S4x15: new triangles



1A2A2B1B2C2D
3A2A2B2C2D2A
2B1C1D3B3C3D

Process fingerprint





Damage



How to break things?

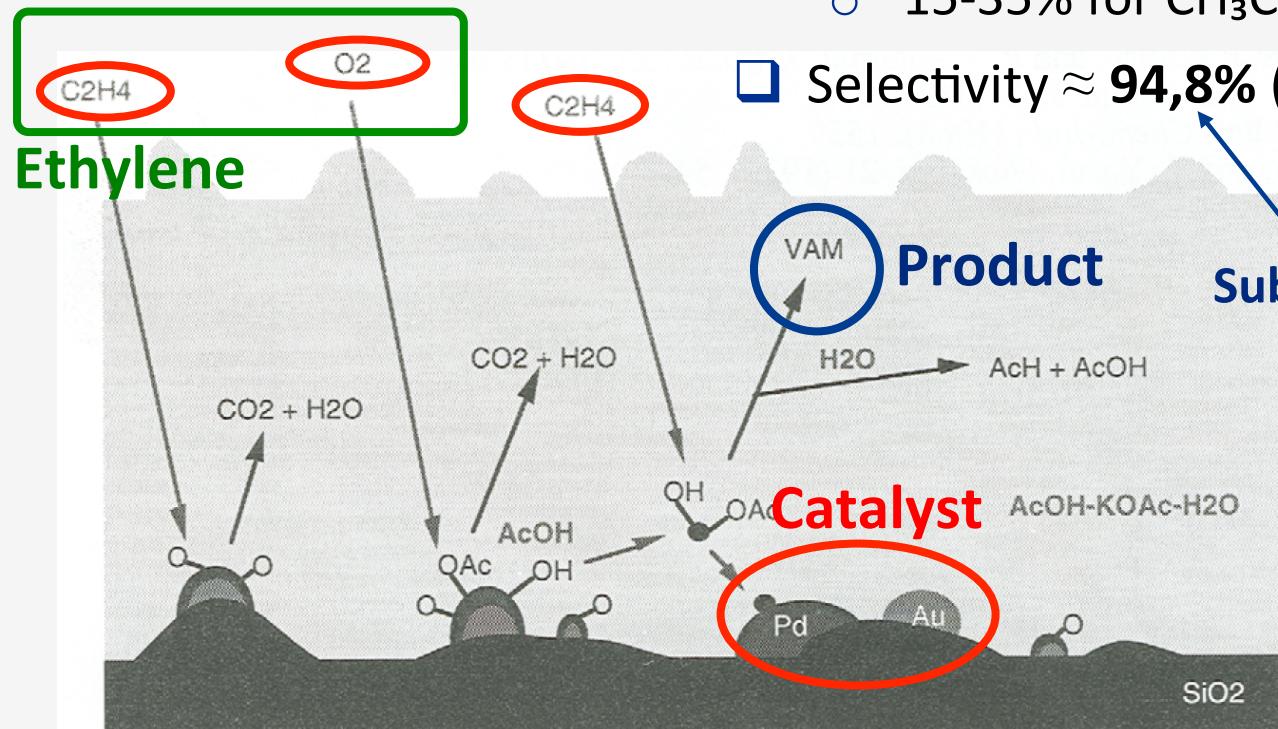


Attacker needs one or more attack scenarios to deploy in final payload

- The least familiar stage to IT hackers
 - In most cases requires input of subject matter experts
- Accident data is a good starting point
 - Governmental agencies
 - Plants' own data bases



Why control before damage?



- Lifetime 1-2 years
- Low per-pass conversion
 - 15-35% for CH_3COOH and 8-10% for C_2H_4
- Selectivity $\approx 94,8\%$ (C_2H_4)

On purpose low

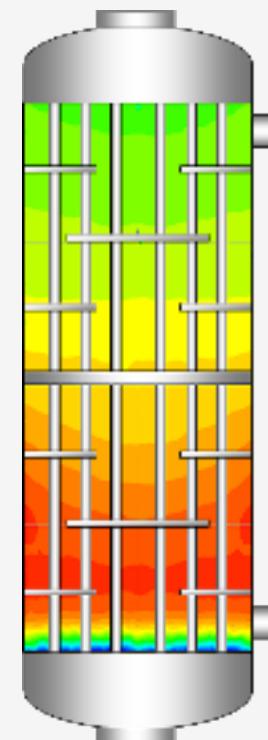
Subjected to constant improvement

Catalyst killers



- Hot spots above 200C -> permanent deactivation
 - Lower activity at T > 180C

We were not able to rise temperature in the reactor and maintain it for long enough to cause damage to the catalyst



Reactor with cooling tubes

Hacker unfriendly process



Target plant may not have been designed in a hacker friendly way

- There may no sensors measuring exact values needed for the attack execution
- The information about the process may spread across several subsystems making hacker invading more devices

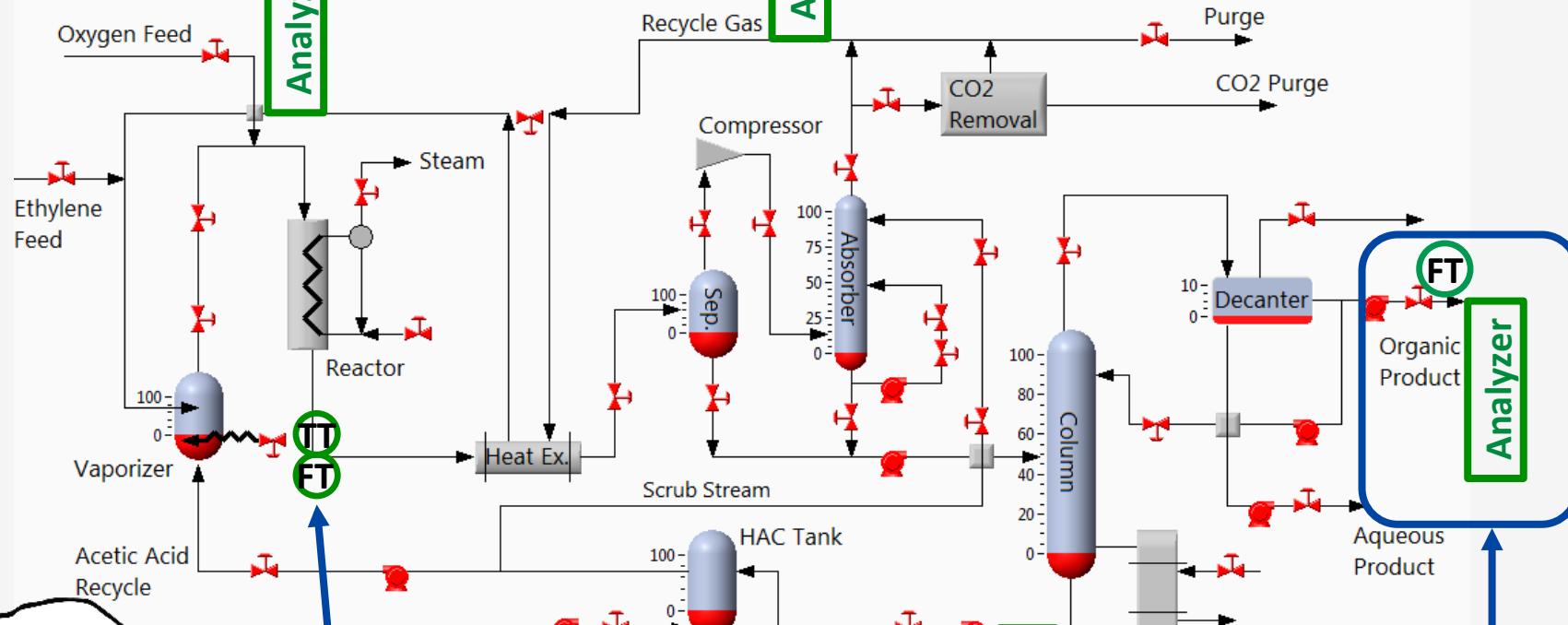


Measuring the process



Chemical composition

Analyzer



- Reactor exit flowrate
- Reactor exit temperature
- No analyzer

Measuring
here is too late

Technician vs. engineer



Technician

“It will eventually drain with the lowest holes loosing pressure last”



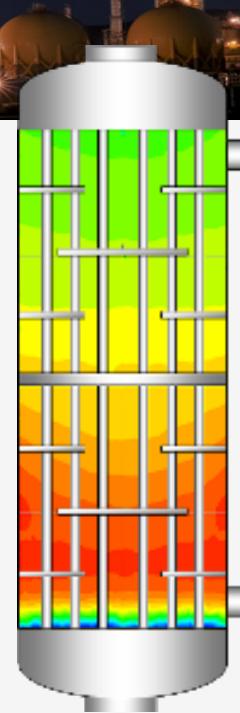
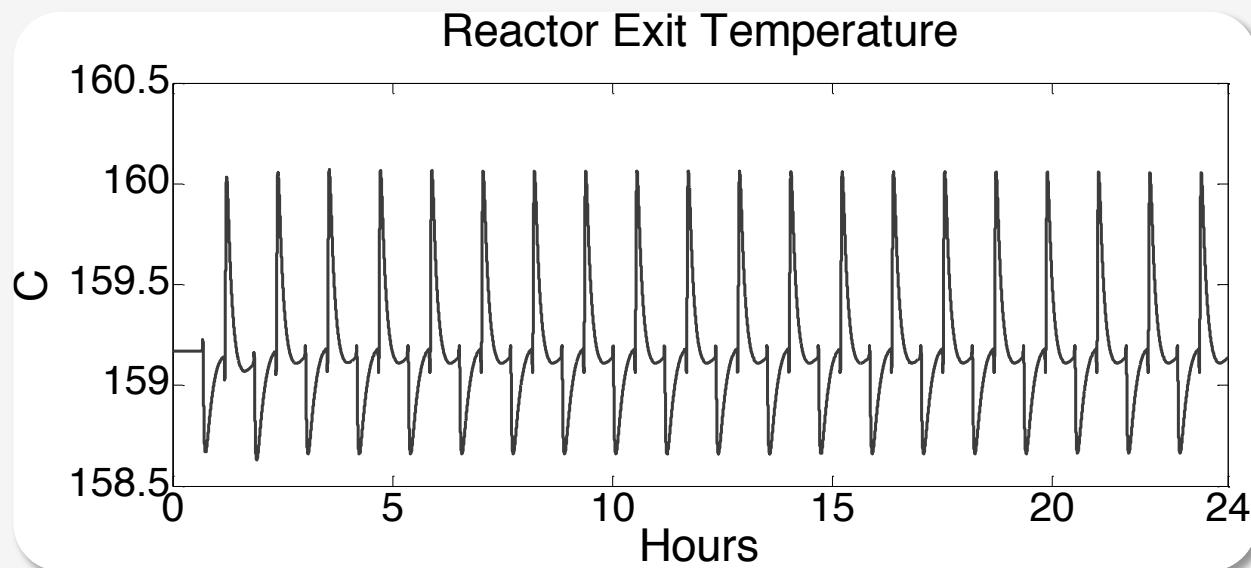
Engineer

“It will be fully drained in 20.4 seconds and the pressure curve looks like this”

Technician answer



Usage of proxy sensor



Reactor with cooling tubes

- Only tells us whether reaction rate increases or decreases
- Is not precise enough to compare effectiveness of different attacks

Quest for engineering answer

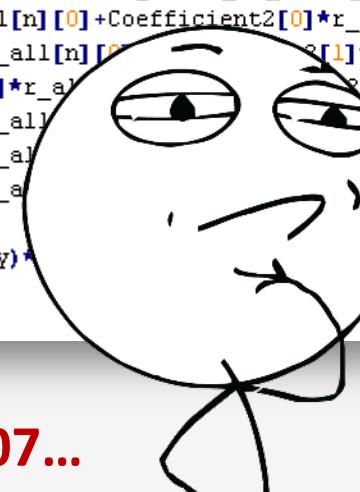


- Code in the controller
- Optimization applications
- Test process/plant

```
/*calculate derivatives*/
for (n=1;n<NR;n++)
{
    /*dC/dt=-delta(C*v)/deltaZ+sum(vij*rj)
    /*Use single backward */ 
    C_O2_t[n-1]=(-(C_O2[n]*v[n]-C_O2[n-1]*v[n-1])/dz + Coefficient1[0]*r_all[n][0]+Coefficient2[0]*r_all[n][1])/cata_porosity;
    C_CO2_t[n-1]=(-(C_CO2[n]*v[n]-C_CO2[n-1]*v[n-1])/dz + Coefficient1[1]*r_all[n][0]+Coefficient2[1]*r_all[n][1])/cata_porosity;
    C_C2H4_t[n-1]=(-(C_C2H4[n]*v[n]-C_C2H4[n-1]*v[n-1])/dz + Coefficient1[2]*r_all[n][0]+Coefficient2[2]*r_all[n][1])/cata_porosity;
    C_VAc_t[n-1]=(-(C_VAc[n]*v[n]-C_VAc[n-1]*v[n-1])/dz + Coefficient1[4]*r_all[n][0]+Coefficient2[4]*r_all[n][1])/cata_porosity;
    C_H2O_t[n-1]=(-(C_H2O[n]*v[n]-C_H2O[n-1]*v[n-1])/dz + Coefficient1[5]*r_all[n][0]+Coefficient2[5]*r_all[n][1])/cata_porosity;
    C_HAc_t[n-1]=(-(C_HAc[n]*v[n]-C_HAc[n-1]*v[n-1])/dz + Coefficient1[6]*r_all[n][0]+Coefficient2[6]*r_all[n][1])/cata_porosity;
    Q_rct[n]= UA*(Tg[n]-Shell_T); /*kcal/min m^3*/
    Tg_t[n-1]=1/(cata_porosity*CCP[n] + cata_heatcapacity *cata_bulk_density)*
    n][1]*E_r2-Q_rct[n]);
}
```

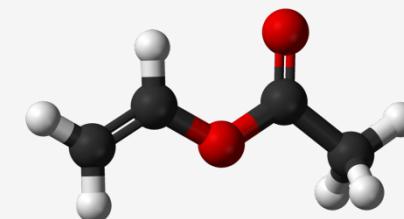
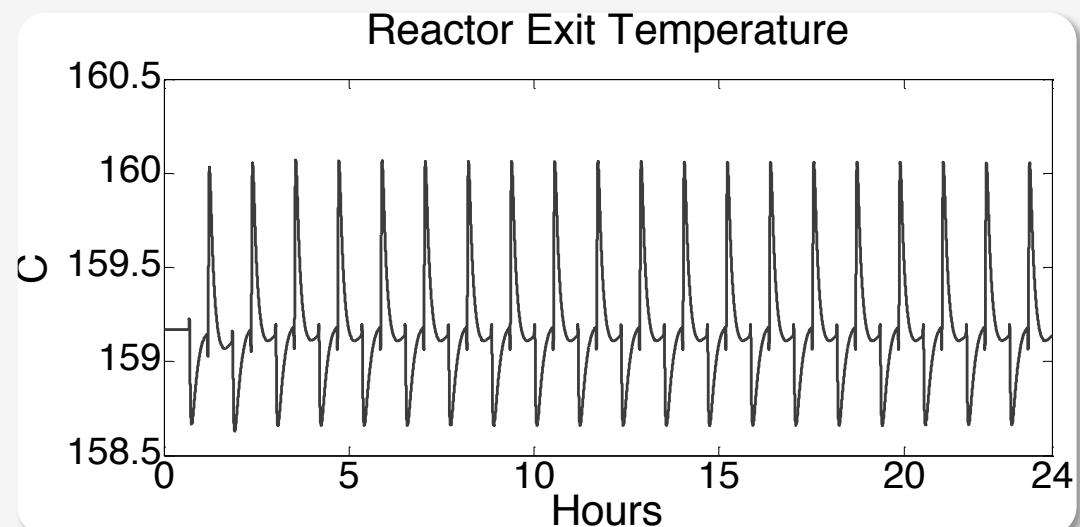
$$(\varepsilon \sum_{k=1}^7 C_{i,k} C p_{i,k} + \rho_b C p_b) \frac{\partial T_i}{\partial t} = - \frac{\partial (\nu_i \sum_{k=1}^7 (C_{i,k} C p_{i,k}) T_i)}{\partial z} - \phi_i \rho_b (r_{1,i} E_1 + r_{2,i} E_2) - Q_i^{RCT}$$

CHALLENGE CONSIDERED

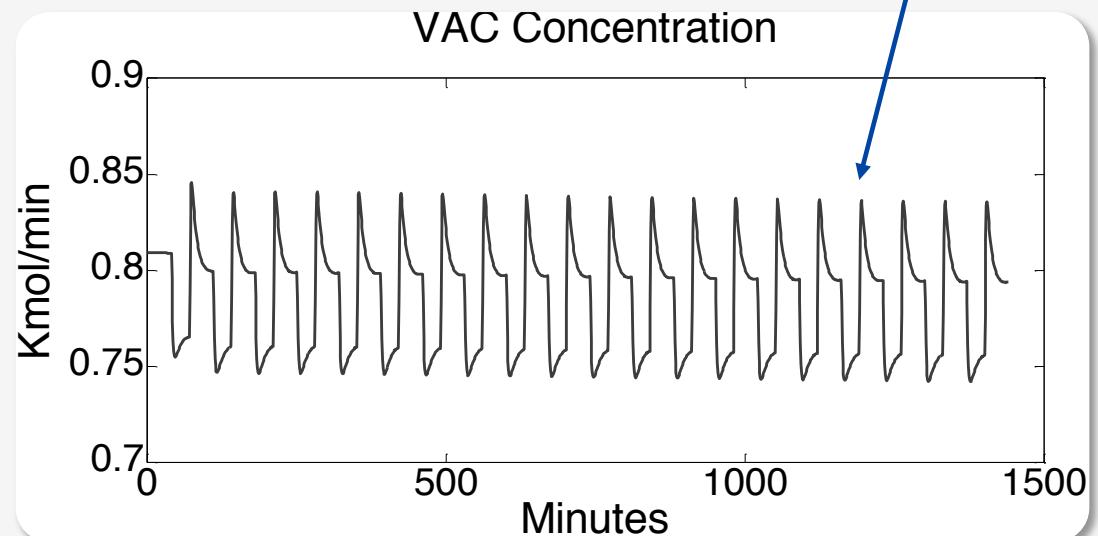


0,00073; 0,00016; 0,0007...

Engineering answer



Vinyl Acetate production

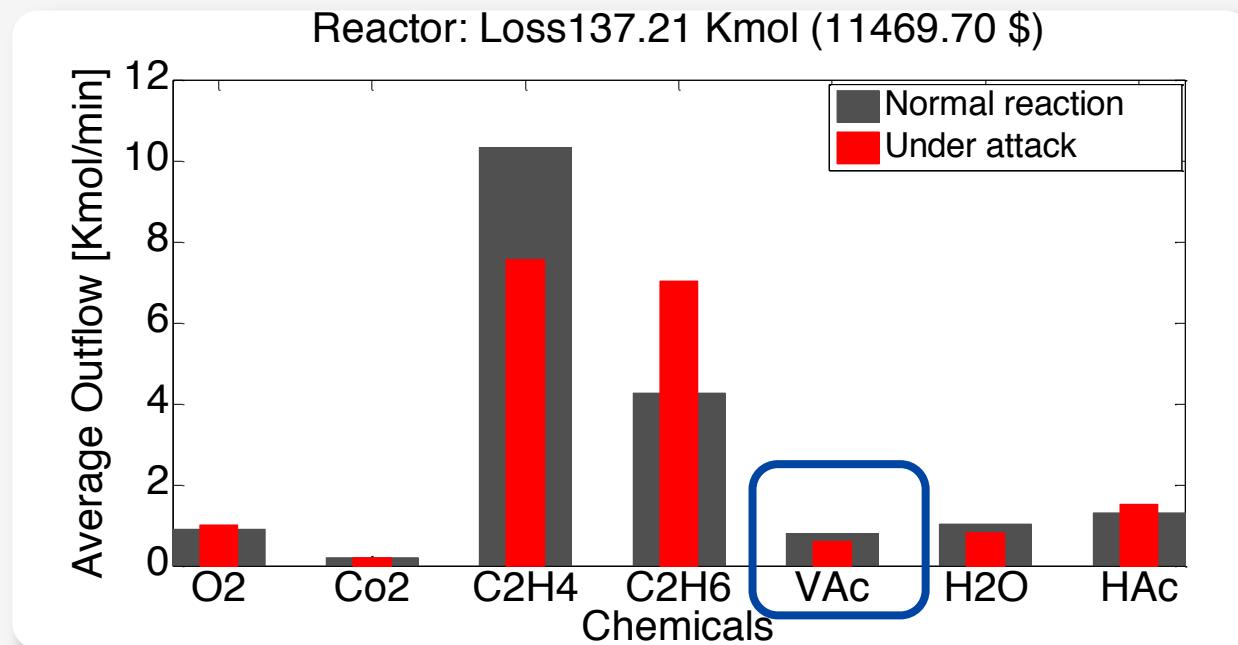


Product loss



Product per day: 96.000\$

Product loss per day: 11.469,70\$



Outcome of the damage stage



Product per day: 96.000\$

Product loss, 24 hours	Steady-state attacks	Periodic attacks
High, $\geq 10.000\$$	XMV {2}	XMV {4;6}
Medium, $5.000\$ - 10.000\$$	XMV {6;7}	XMV {5;7}
Low, $2.000\$ - 5.000\$$	-	XMV {2}
Negligible, $\leq 2.000\$$	XMV {1;3}	XMV {1;2}

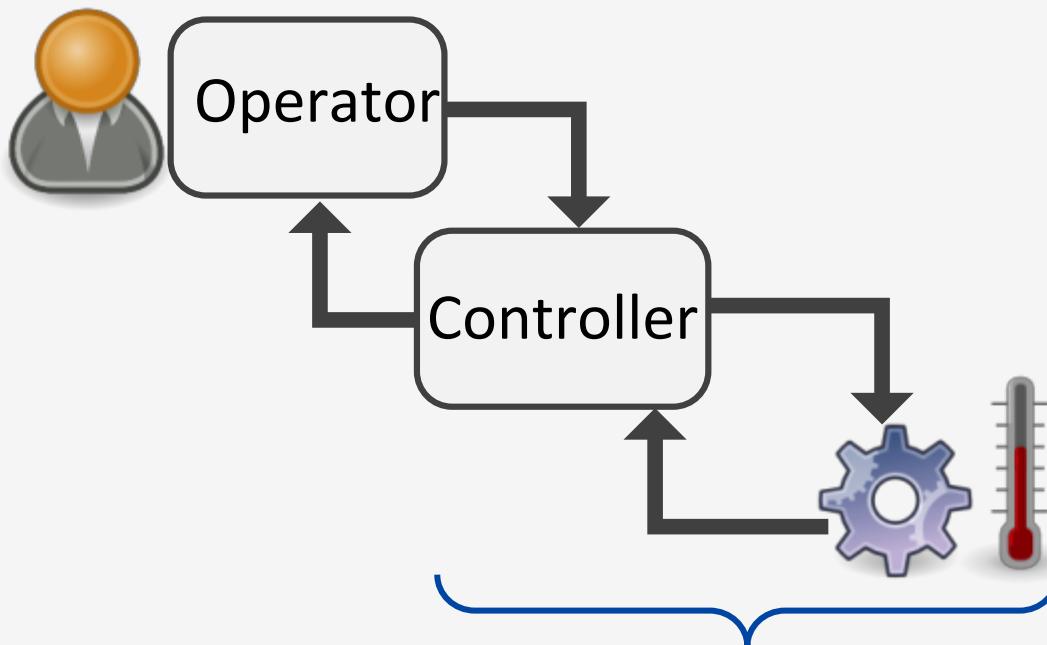
Still might be useful



Clean-up



Socio-technical system



- Maintenance stuff
- Plant engineers
- Process engineers
-

Creating forensics footprint

- ❑ Process operators may get concerned after noticing persistent decrease in production and may try to fix the problem
- ❑ If attacks are timed to a particular employee shift or maintenance work, plant employee will be investigated rather than the process



Creating forensics footprint



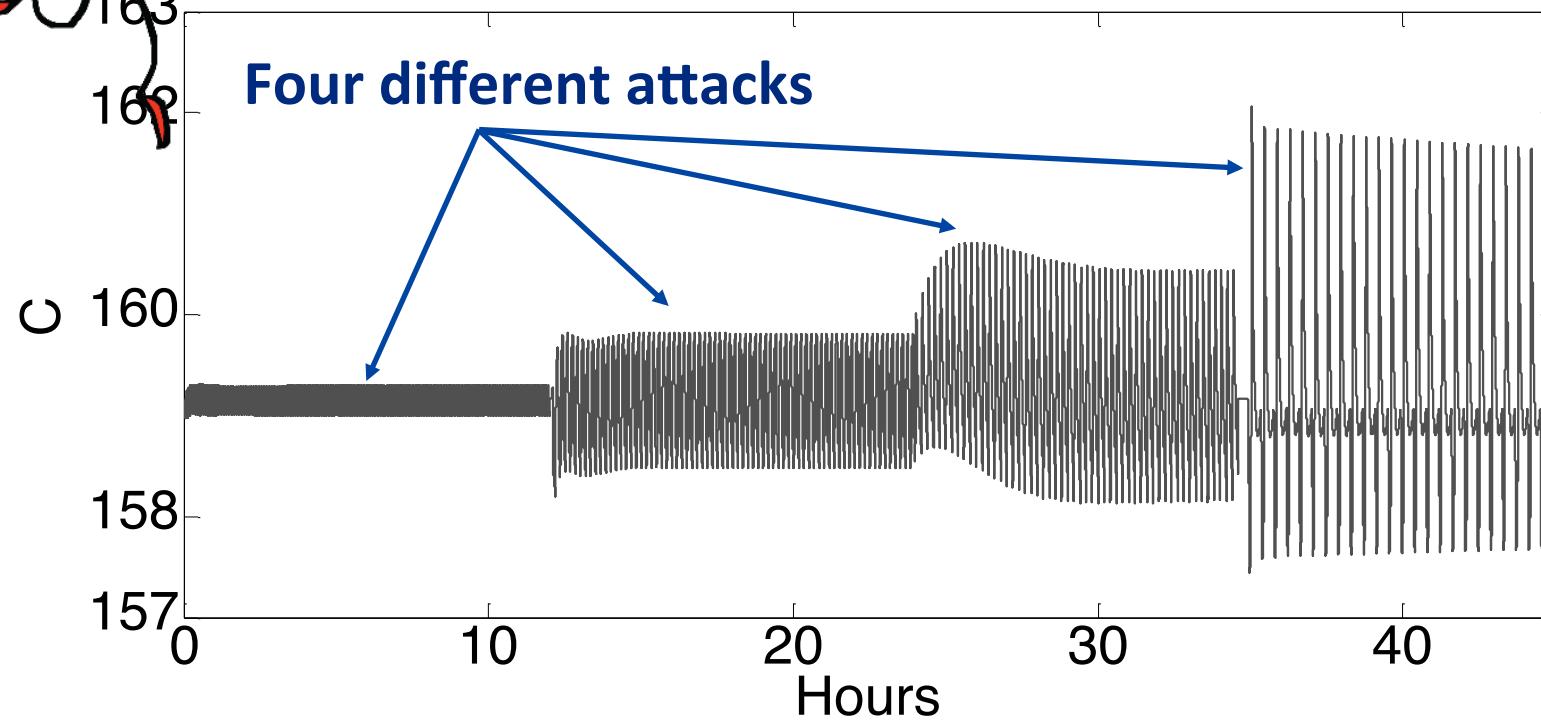
1. Pick several ways that the temperature can be increased
2. Wait for the scheduled instruments calibration
3. Perform the first attack
4. Wait for the maintenance guy being yelled at and recalibration to be repeated
5. Play next attack
6. Go to 4



Creating forensics footprint



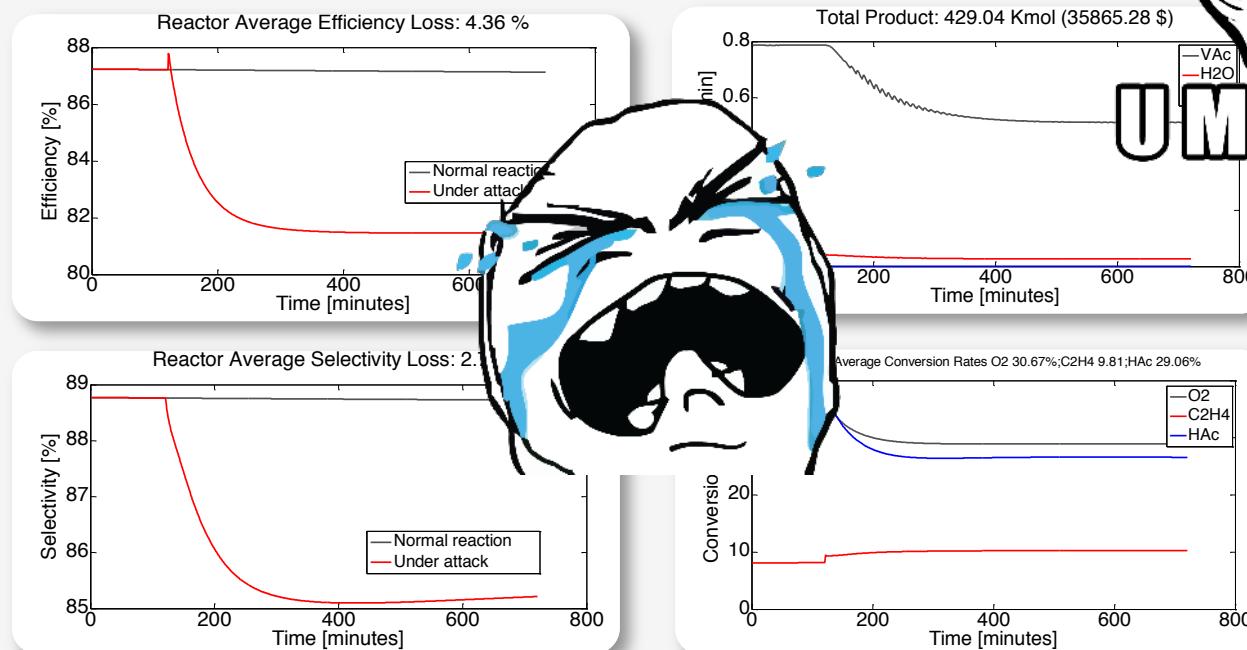
Reactor Temperature



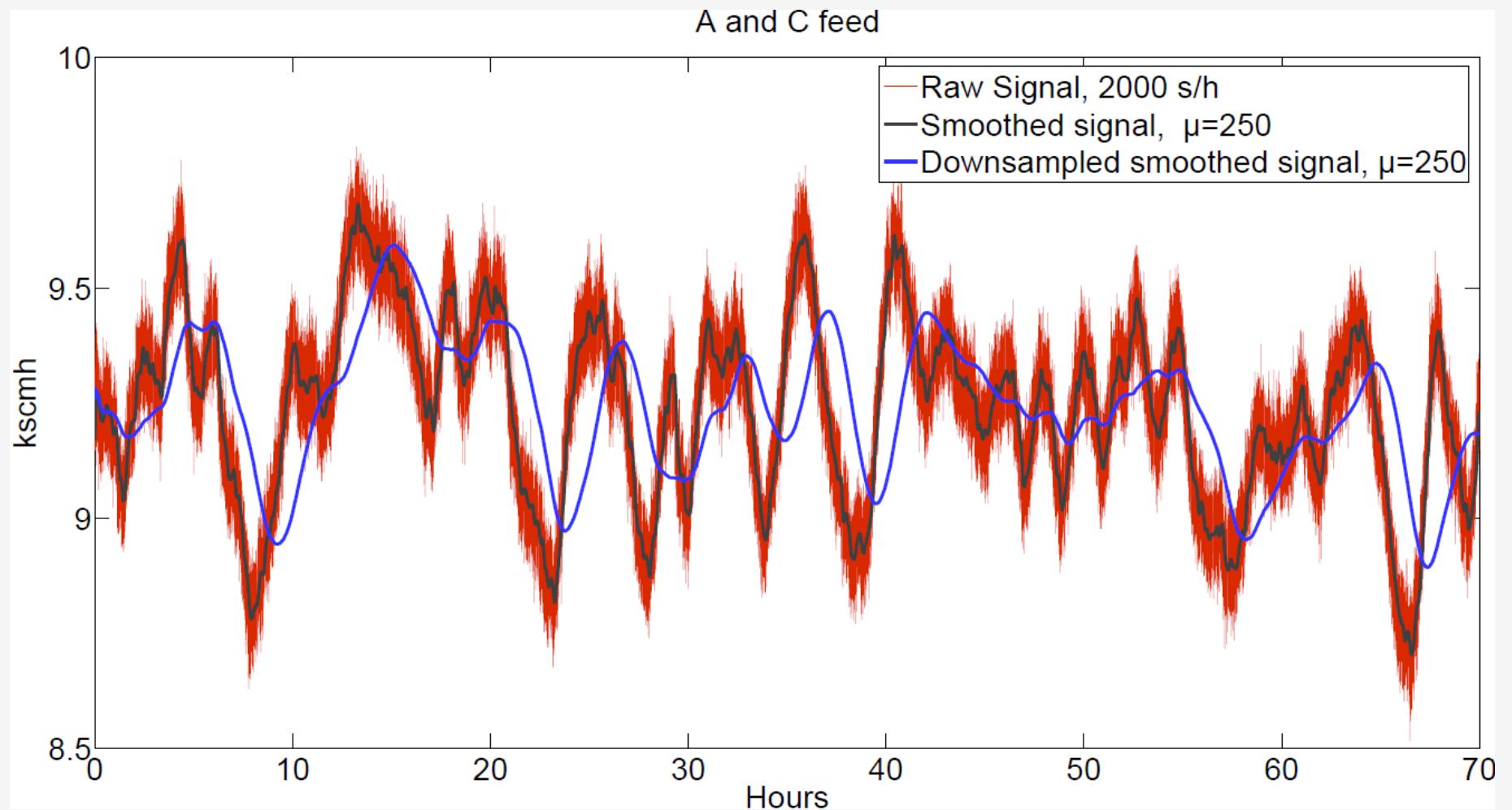
Defeating chemical forensics

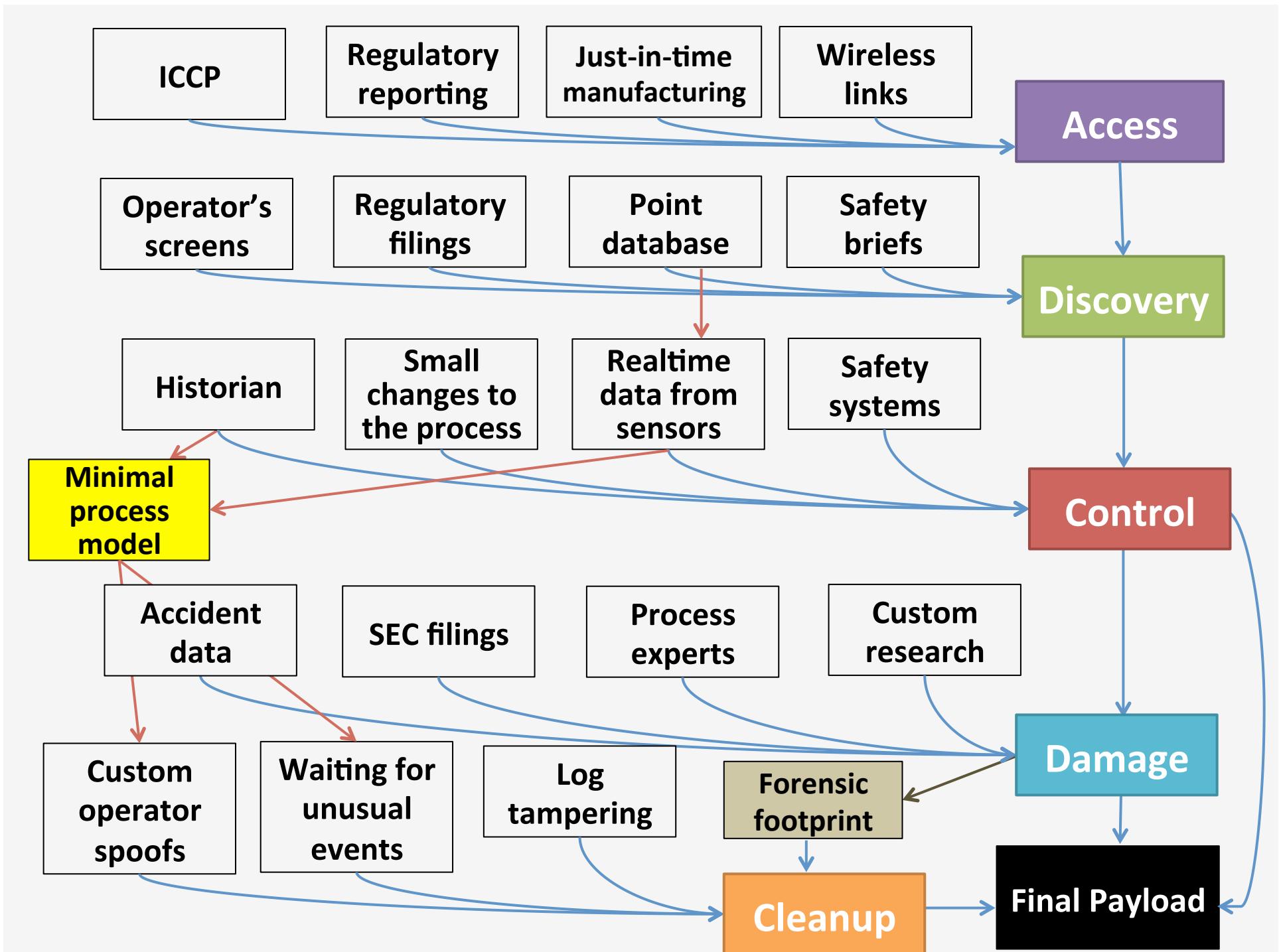


- ❑ If reactor deemed malfunctioning, chemical forensics will be asked to assist
- ❑ Change attack patterns according to debugging efforts of plant personnel



Data synchronization and processing

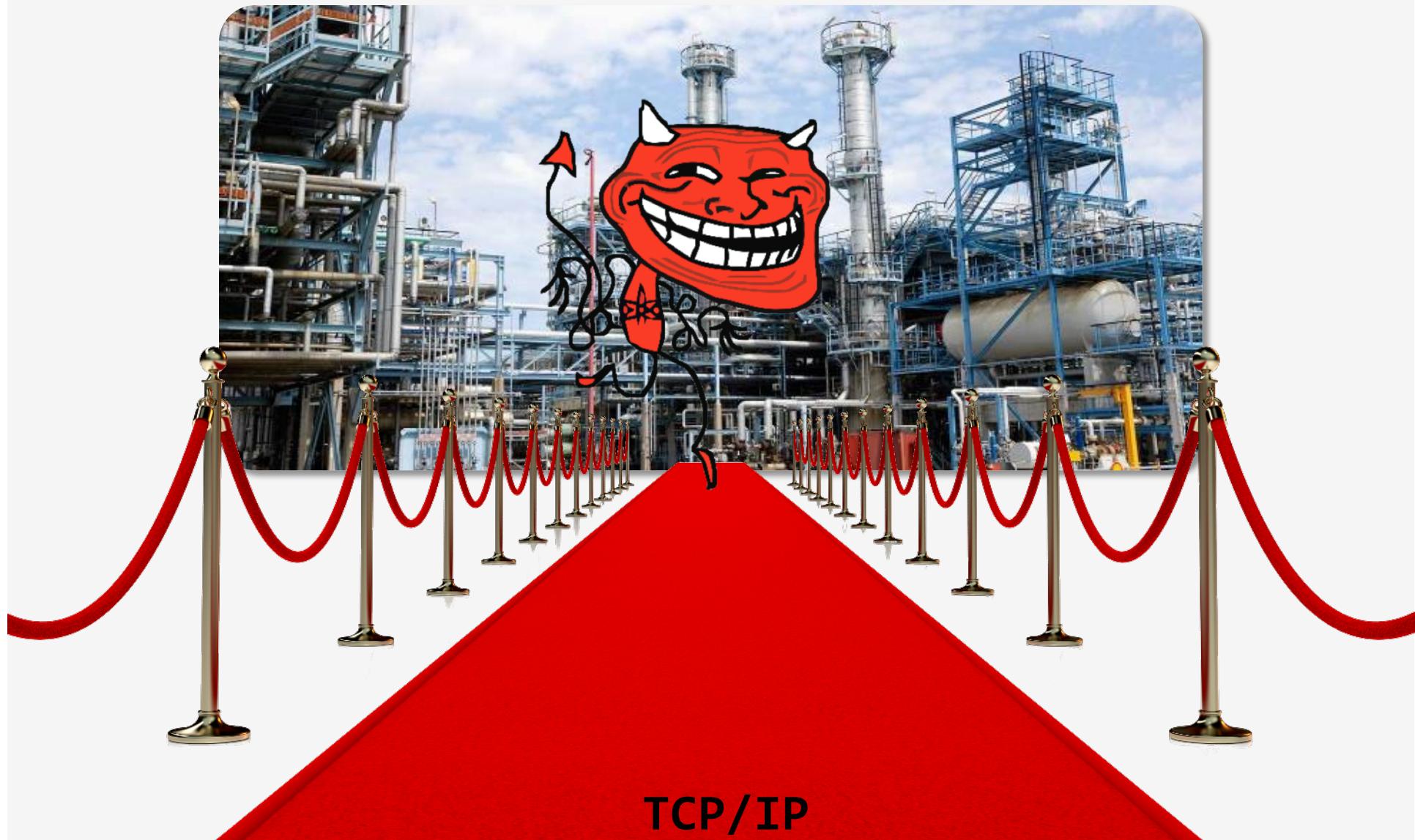






Afterword

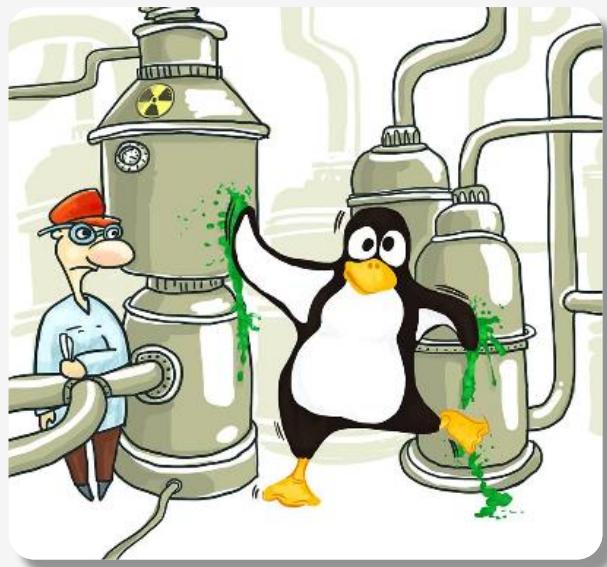
State-of-the-art of ICS security



Food for thought



- ❑ **Cost of attack can quickly exceed cost of damage**
 - Hacking into large number of devices
 - Suppression of alarms and process data spoofing
 - Badly behaved control loops , synchronization of actions
- ❑ **Each process is unique, but...**
 - There are instances of attacks applicable to wide range of scenarios
 - **SCADA payloads for Metasploit is just a matter of time**



Thank you
marina.krotofil@tuhh.de
@marmusha

Damn Vulnerable Chemical Process

TE: <http://github.com/satejnik/DVCP-TE>

VAM: <http://github.com/satejnik/DVCP-VAM>

Thanksgiving:
Jason Larsen for all collaborations